SUMÁRIO EXECUTIVO

LEVANTAMENTO DA TECNOLOGIA *blockchain*

2020

TRIBUNAL DE CONTAS DA UNIÃO

REPÚBLICA FEDERATIVA DO BRASIL

TRIBUNAL DE CONTAS DA UNIÃO

MINISTROS

José Mucio Monteiro, **Presidente**

Ana Arraes, **Vice-Presidente**
Walton Alencar Rodrigues
Benjamin Zymler
Augusto Nardes
Aroldo Cedraz de Oliveira
Raimundo Carreiro
Bruno Dantas
Vital do Rêgo

MINISTROS-SUBSTITUTOS

Augusto Sherman Cavalcanti
Marcos Bemquerer Costa
André Luís de Carvalho
Weder de Oliveira

MINISTÉRIO PÚBLICO JUNTO AO TCU

Cristina Machado da Costa e Silva, **Procuradora-Geral**
Lucas Rocha Furtado, **Subprocurador-Geral**
Paulo Soares Bugarin, **Subprocuradora-Geral**
Marinus Eduardo de Vries Marsico, **Procurador**
Júlio Marcelo de Oliveira, **Procurador**
Sergio Ricardo Costa Caribé, **Procurador**
Rodrigo Medeiros de Lima, **Procurador**

SUMÁRIO EXECUTIVO

LEVANTAMENTO DA TECNOLOGIA *blockchain*

BRASÍLIA, 2020

TRIBUNAL DE CONTAS DA UNIÃO

Brasil. Tribunal de Contas da União.

Levantamento da tecnologia blockchain / Tribunal de Contas da União; Relator Ministro Aroldo Cedraz. – Brasília: TCU, Secretaria das Sessões (Seses), 2020.

39 p. : il. – (Sumário Executivo)

Conteúdo relacionado ao Acórdão 1.613/2020-TCU-Plenário, sob relatoria do Ministro Aroldo Cedraz.

1. Prestação de contas. 2. Tecnologia disruptiva.

3. Blockchains. 4.Bitcoin.

I. Título. II. Série.

Ficha catalográfica elaborada pela Biblioteca Ministro Ruben Rosa


0.78
0.89
0.45
0.89
0.89

_APRESENTAÇÃO

O termo *blockchain* tem sua origem em 2008, quando um autor desconhecido de codinome Satoshi Nakamoto publicou o documento intitulado *"Bitcoin: A Peer-To--Peer Electronic Cash System"* em uma lista de discussão na internet. O referido documento apresenta uma combinação criativa de diversos conceitos relacionados à computação que permitem realizar pagamentos on-line sem a necessidade de uma terceira parte confiável: redes *peer-to-peer (P2P*), serviço de *timestamp* distribuído, criptografia, assinatura digital, árvore de *merkle,* funções *hash* e ponteiros de *hash*, além de outras inovações.

Nota-se que o Bitcoin é a primeira e mais famosa aplicação baseada em *blockchain*. Mas esses conceitos não devem ser confundidos. A *blockchain* é um conceito tecnológico, enquanto o Bitcoin é um dos casos de uso para um tipo específico da tecnologia *blockchain*. Curiosamente, o termo blockchain não foi mencionado explicitamente no artigo elaborado por Nakamoto, mas o conceito de uma estrutura encadeada de *hashes* criptográficos (ou resumos criptográficos), na qual cada elemento faz referência ao *hash* do bloco anterior, surgiu no artigo original do *Bitcoin.*

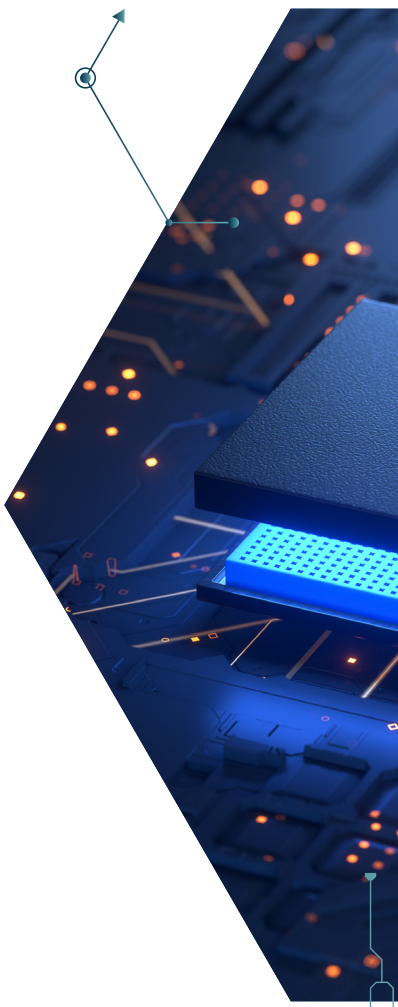
Importante notar que a *blockchain* do *Bitcoin* proposta por Nakamoto só possibilitava transações monetárias. Desta forma, não havia como adicionar condições mais elaboradas a essas transações. Em 2013, Vitalik Buterin propôs uma plataforma para o desenvolvimento de aplicações descentralizadas chamada *Ethereum*. Com o suporte para contratos inteligentes (em inglês, *Smart Contracts),* elevou-se a um novo patamar a tecnologia *blockchain*, uma vez que agora era possível executar, de forma autônoma e confiável, um código (ou programa) acordado previamente por duas ou mais partes.

> Todos esses conceitos reunidos fazem com que a *blockchain* seja considerada uma tecnologia disruptiva, devido à sua capacidade de digitalizar, proteger e rastrear transações sem a necessidade de uma terceira parte confiável, o que se traduz no fato de diversas aplicações descentralizadas poderem ser desenvolvidas.

A *blockchain* também pode ser enquadrada como uma tecnologia de propósito geral, ou seja, uma tecnologia com características únicas e capazes de impactar drasticamente as relações econômicas e sociais pré-existentes, bem como prover significativas melhorias e facilitar a criação de inovações em diversos setores da economia.

Destaca-se que a transformação tecnológica vai além da inovação trazida pelas *blockchains* do *Bitcoin* e da *Ethereum*. Segundo a empresa de consultoria Gartner, até 2023 a tecnologia blockchain suportará o movimento global e rastreamento de dois trilhões de dólares de bens e serviços anualmente. A empresa de consultoria também afirma que a blockchain tem, no mínimo, o potencial de otimizar e, possivelmente, transformar, de forma disruptiva, os serviços públicos.

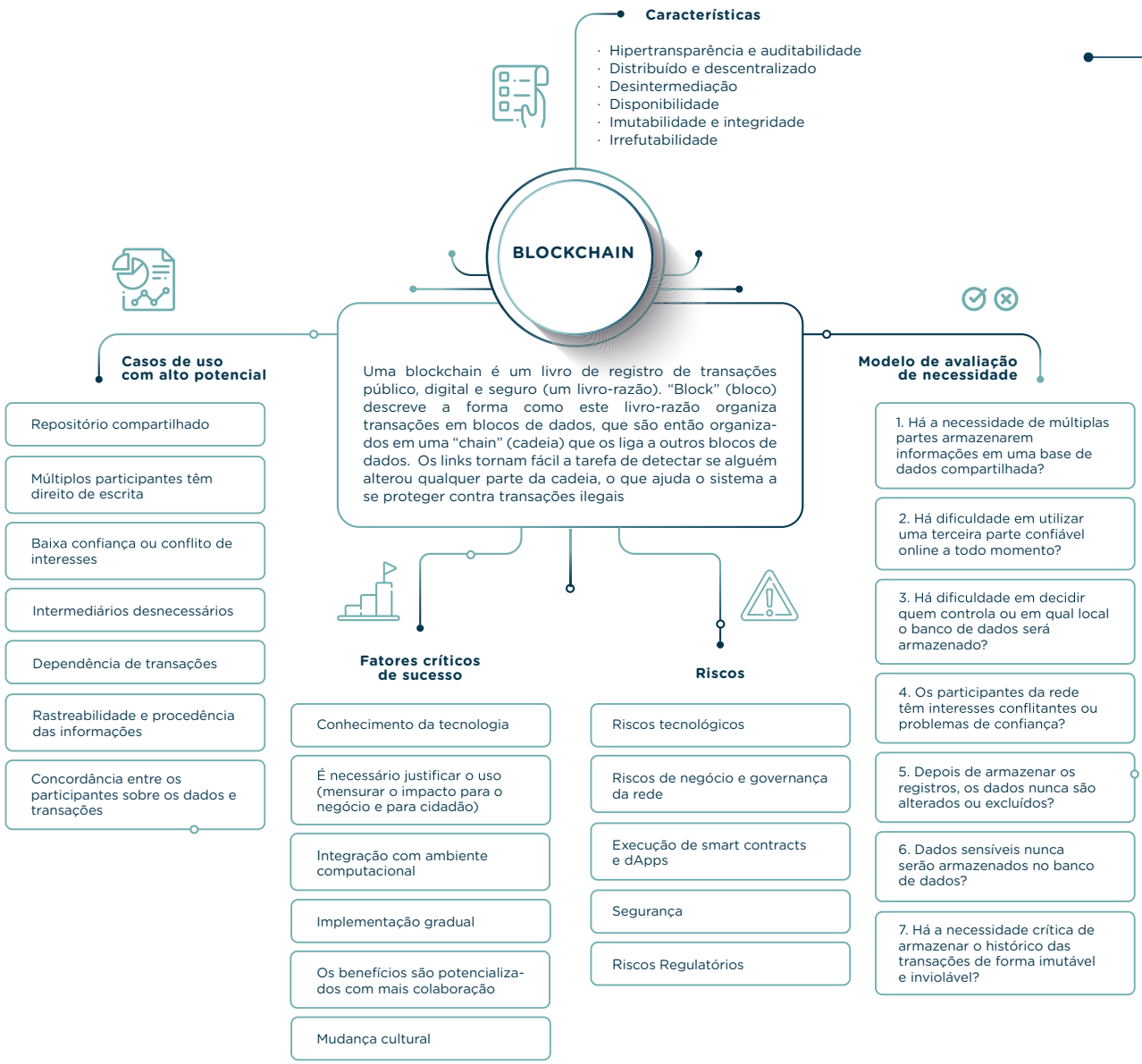
O uso da tecnologia *blockchain* é indicado quando há necessidade de aumentar a confiabilidade de informações e processos em situações que envolvem muitas partes interessadas e heterogêneas. Por meio de trilhas de auditoria confiáveis, é possível rastrear todas as operações sobre os dados que são armazenados em um livro-razão digitalizado na internet, aumentando a transparência e aperfeiçoando o processo de prestação de contas.



Todavia, deve-se considerar que a empolgação gerada por uma nova tecnologia pode acarretar o desperdício de dinheiro público, especialmente quando a tecnologia não é totalmente compreendida pelos gestores e as incertezas não são consideradas. Tecnologias inovadoras surgem com frequência e os governos precisam estar preparados para lidar com os novos riscos e aproveitar as oportunidades que são abertas.

Bem como. o presente Sumário Executivo, relativo ao Acórdão 1.613/2020-TCU-Plenário, sob relatoria do Ministro Aroldo Cedraz, tem o intuito de compreender o que são as tecnologias *blockchain* e de livros-razão distribuídos (*Distributed Ledger Technology - DLT*), assim como analisar o potencial e as incertezas dessas tecnologias para os serviços digitais do governo.

FIGURA 1 – FRAMEWORK PARA IMPLEMENTAR A TECNOLOGIA *BLOCKCHAIN*



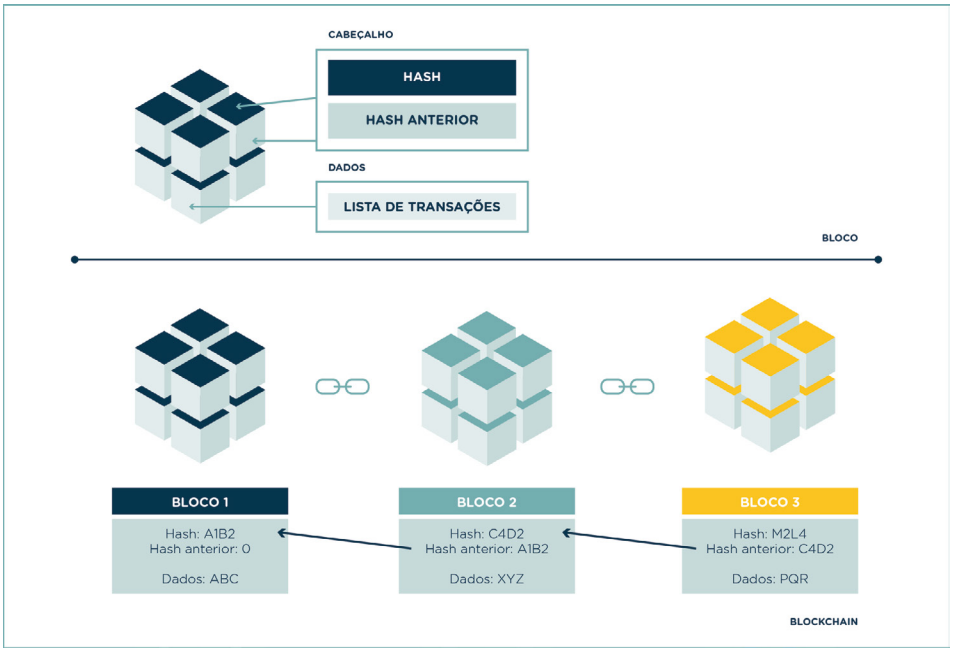
_SUMÁRIO

1_ BLOCKCHAIN E DISTRIBUTED LEDGER TECHNOLOGY (DLT)

Segundo a Organização para a Cooperação e Desenvolvimento Econômico (OCDE), a tecnologia *blockchain* é uma forma de tecnologia distribuída de livro-razão, a qual atua como um registro (uma lista) aberto e autenticado de transações de uma parte para outra (ou múltiplas partes), que não são armazenadas por uma autoridade central. Em vez disso, cada usuário armazena uma cópia local do livro-razão, executando um *software blockchain* conectado a uma rede *blockchain* – também conhecido como nó. Ao invés de uma autoridade central manter exclusivamente a base de dados, todos os nós têm uma cópia do livro-razão, sendo que as atualizações do livro-razão *blockchain* são propagadas através da rede em minutos ou segundos.

Sob um aspecto mais técnico, uma *blockchain* é uma estrutura de dados que armazena transações organizadas em blocos, os quais são encadeados sequencialmente, servindo como um sistema de registros distribuído. Cada bloco é dividido em duas partes: cabeçalho e dados. O cabeçalho inclui metadados como um número único que referencia o bloco, o horário de criação do bloco e um apontador para o *hash* do bloco anterior, além do *hash* próprio do bloco. Os dados geralmente incluem uma lista de transações válidas e os endereços das partes, de modo que é possível associar uma transação às partes envolvidas (origem e destino). A figura abaixa ilustra como os blocos são sequenciados na *blockchain*.

FIGURA 2 – ENCADEAMENTO DE BLOCOS NA BLOCKCHAIN

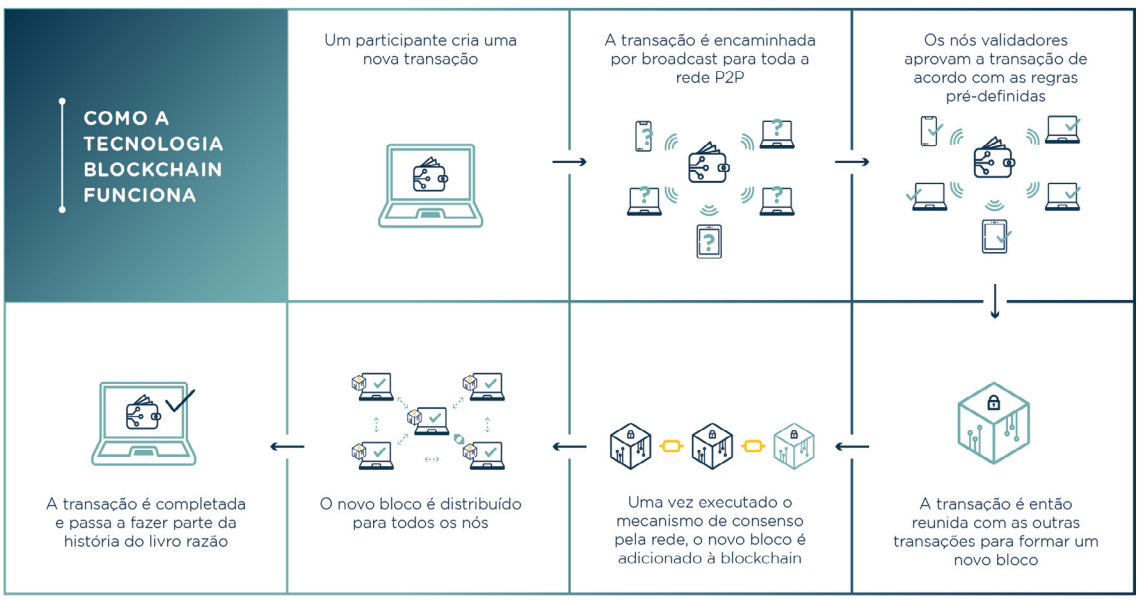


FONTE: THE INTERNATIONAL TELECOMMUNICATION UNION - ITU (ADAPTADO)

Como se observa, cada novo bloco incluído na cadeia possui um conjunto de transações e uma identificação única, gerada a partir de um resumo criptográfico de *hash*. O cabeçalho possui um campo que armazena o resumo criptográfico (*hash)* do bloco imediatamente anterior, estabelecendo uma sequência única entre os blocos. Como cada bloco faz referência ao seu antecessor, se um *bit* do bloco anterior é alterado, o *hash* do bloco muda e consequentemente há uma inconsistência na cadeia, que pode ser facilmente detectável. Por esse motivo, assume-se que a existência em uma cadeia de blocos interligados garante a segurança e integridade das transações armazenadas.

A transação é a abstração de um evento de negócios que altera o estado de um livro-razão. Uma plataforma *blockchain* facilita a execução segura de uma transação no ambiente descentralizado e auditável. A figura abaixo resume o funcionamento genérico de como uma transação é realizada em uma *blockchain.*

FIGURA 3 - FUNCIONAMENTO GENÉRICO DE UMA *BLOCKCHAIN*



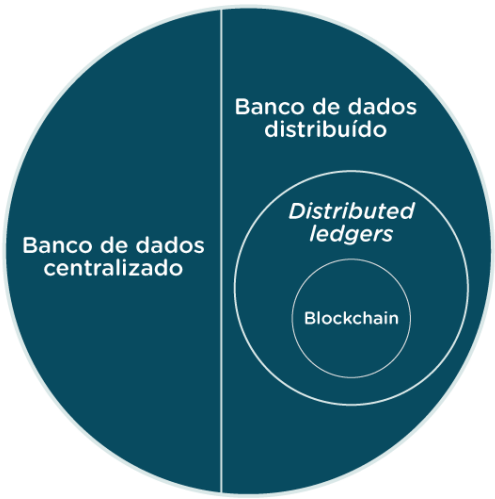
FONTE: COMISSÃO EUROPEIA (ADAPTADO)

Conceitualmente, uma *blockchain* é um caso específico de uma *DLT*, embora esses dois termos sejam frequentemente utilizados de forma intercambiável em diversos documentos pesquisados.

A Comissão Europeia define *DLT* como uma tecnologia que facilita a expansão de registros transacionais inalteráveis, assinados criptograficamente em uma lista ordenada cronologicamente e compartilhada por todos os participantes da rede. Qualquer participante com direito de acesso pode rastrear a origem de um evento transacional,

em qualquer ponto de sua história, pertencente a qualquer ator da rede. A tecnologia armazena transações de uma forma descentralizada. Transações com troca de valores são executadas diretamente entre pares *(peers)* conectados e são verificadas consensualmente, aplicando-se algoritmos na rede. O diagrama a seguir exemplifica a diferença entre banco de dados tradicional, *DLT* e *blockchain*.

FIGURA 4 - DIFERENÇA ENTRE TECNOLOGIAS



Banco de dados distribuído

- não existe um "*master database*" central;
- provê um grau de tolerância a falhas caso alguns nós falhem;
- banco de dados tradicionais são, em geral, operados por uma entidade única que mantém um estrito controle de acesso para a rede;

***Distributed Ledger Technology* (DLT)**

- mecanismo de consenso é baseado em um modelo de ameaças de adversários, assumindo que nem todos participantes são honestos;
- o banco de dados deve ser capaz de sincronizar e executar mesmo se um certo número de nós estão agindo de forma maliciosa;
- nós individuais precisam ser capazes de: **a)** verificar e validar, de forma independente, transações que alteram o estado do banco de dados e **b)** recriar todo o histórico de transações, de forma independente;

Blockchain

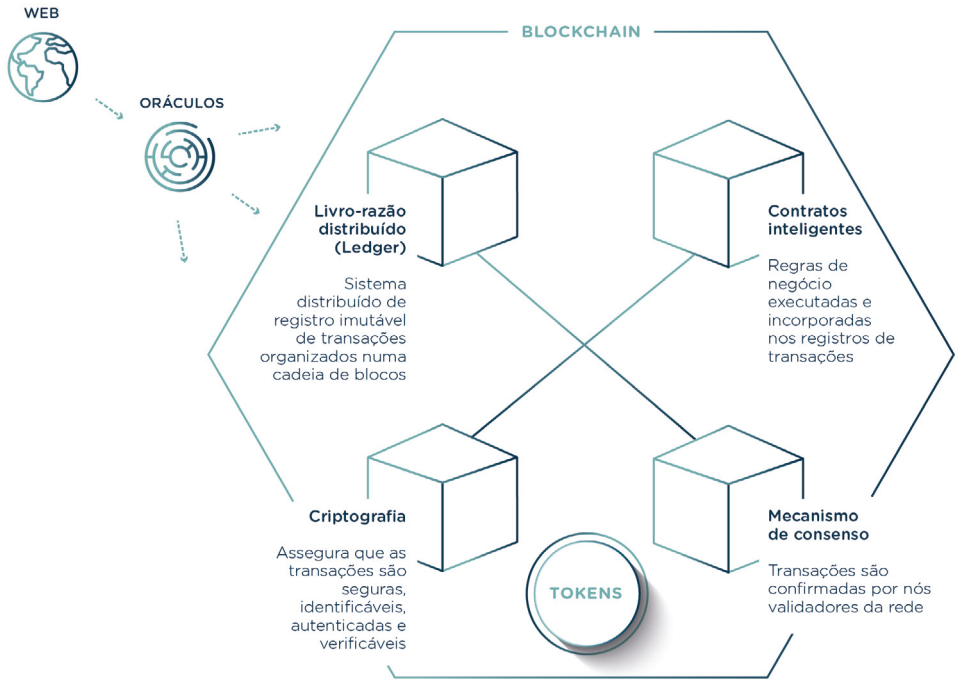
- usa uma estrutura de dados especial, *append-only*, que é composta por transações em lotes de blocos, os quais são ligados sequencialmente de forma inviolável, determinando a ordem das transações no sistema;

FONTE: UNIVERSIDADE DE BERKELEY E FÓRUM ECONÔMICO MUNDIAL (ADAPTADOS)

2_ COMPONENTES DA TECNOLOGIA *BLOCKCHAIN*

As implementações da tecnologia *blockchain* incluem tipicamente os seguintes componentes, que serão detalhados a seguir.

FIGURA 5 - COMPONENTES DA TECNOLOGIA *BLOCKCHAIN*



2.1 LIVRO-RAZÃO DISTRIBUÍDO (LEDGER)

O livro-razão *(ledger)* é a estrutura de dados imutável, em que transações são registradas e o estado global do sistema é mantido. O livro-razão mantém-se completamente replicado, via de regra, em todos os nós da rede *P2P*. Logo, o livro-razão distribuído é replicado e imutável.

Um livro-razão distribuído pode ser visto como um registro de transações ou contratos mantidos de forma descentralizada em diferentes locais, eliminando a necessidade de uma autoridade central para controlar o armazenamento dos dados.

Enquanto um livro-razão centralizado está propenso a diversos ataques cibernéticos, um livro-razão distribuído é mais difícil de atacar, porque todas as cópias distribuídas precisam ser atacadas simultaneamente para que um ataque seja bem-sucedido. Além disso, os registros distribuídos são resistentes a alterações maliciosas por um único participante da rede.

Destaca-se que o elemento de descentralização das tecnologias de livro-razão distribuído cria um sistema no qual todas as transações são compartilhadas, verificadas e aceitas por todas as partes, eliminando a necessidade de intermediários.

2.2 MECANISMOS DE CONSENSO

Considerando que as primeiras aplicações de *blockchain* são redes públicas e anônimas, como garantir que os usuários dessas redes se comportem de forma honesta? Deve haver uma forma coordenada em que todas as transações sejam validadas e os nós participantes cheguem a um acordo em relação ao estado da rede. Daí surgem os chamados mecanismos de consenso, que são as regras e os procedimentos pelos quais os nós de uma rede distribuída concordam em validar transações. Importante notar que acréscimos no livro-razão só são feitos se as regras ditadas pelo mecanismo de consenso forem seguidas por todos.

Especificamente em uma rede *blockchain*, o consenso é obtido por meio da convergência dos nós em direção a uma versão única e imutável do livro-razão. O mecanismo de consenso é responsável por permitir que os atores ou nós da rede concordem entre si com o conteúdo a ser armazenado na *blockchain*, levando em consideração o fato de que alguns atores podem ser maliciosos ou estar indisponíveis. Isso pode ser atingido por diferentes maneiras, conforme as necessidades específicas de cada rede.

Importante notar que, para uma transação ser registrada em um livro-razão, ela primeiro precisa ser aprovada pelos nós validadores da rede, caso contrário, é automaticamente rejeitada, o que ocorre da seguinte maneira: sempre que uma transação é encaminhada à rede *P2P,* os nós primeiramente validam a transação segundo regras pré-definidas. Se os nós concordam com sua legitimidade, a transação é encaminhada para os outros nós validadores da rede e aguardam em um *pool* de transações. Um aspecto fundamental da tecnologia distribuída é determinar qual participante adicionará o próximo bloco. Assim que um nó é eleito ou torna-se apto a criar um bloco, este novo bloco é adicionado à cadeia anterior de blocos de forma imutável, contendo as transações mantidas em seu *pool*. Desta maneira, a sequência de blocos mais recente mantém uma visão compartilhada e acordada do estado atual da *blockchain.*

Cada algoritmo de consenso tem diferentes configurações de conflitos de escolhas *(trade-offs)*, que são otimizados para atender uma determinada necessidade. Cabe ao gestor avaliar que tipo de problema distribuído precisa resolver com a utilização de solução *DLT* ou *blockchain*, a fim de selecionar o mecanismo de consenso que se ajusta ao seu ambiente, em termos de escalabilidade do número de nós e transações, bem como quais e quantos serão os participantes da rede.

2.3 CONTRATOS INTELIGENTES

Um contrato celebrado entre partes interessadas usualmente tem um conjunto de cláusulas (promessas) que são pactuadas e assinadas entre as partes. Contratos são, geralmente, escritos pelas partes envolvidas, autenticados e auditados por entidades intermediárias. Intermediários como advogados, cartórios (tabeliões), corretores, auditores e empresas são responsáveis por estabelecer uma relação de confiança entre as partes. No caso de cartórios, o próprio contrato fica registrado em um ente intermediário, que detém sua custódia e dá fé pública ao documento. A principal razão para a existência de tais intermediários é a necessidade de mediação entre partes que não têm uma relação de confiança entre si.

Contratos inteligentes, ou *smart contracts*, são código-fonte em linguagem de programação *(scripts)*, que podem ser definidos e auto executados em uma infraestrutura de *blockchain* ou *DLT*. A definição e execução de um contrato inteligente nesses ambientes se dá sem a necessidade de intermediários.

O conceito de contrato inteligente foi definido por Nick Szabo, pesquisador em criptografia e especialista em Direito. Em seus artigos, Szabo define contrato inteligente como cláusulas contratuais embutidas em *hardware* e *software* de violação proibitiva, sob o ponto de vista computacional e, consequentemente, econômico, portanto, não vantajosa a um possível violador.

Um outro conceito dado pela *International Telecommunication Union (ITU)* é que contrato inteligente é um programa de computador que utiliza transações assinadas criptograficamente em uma rede *DLT.* O contrato inteligente é executado pelos nós e os resultados da execução são validados por consenso e registrados no livro-razão distribuído. A automação inteligente de contratos reduz custos e riscos de erros, mitiga riscos de fraude e, potencialmente, otimiza muitos processos de negócios.

Ainda segundo Szabo, um contrato inteligente pode ser caracterizado pelo atingimento de quatro objetivos principais:

a. observabilidade: a habilidade de verificar se as partes envolvidas no contrato cumpriram sua parte;

b. verificabilidade: a possibilidade de uma das partes envolvidas reclamar que o contrato foi cumprido ou violado;

c. privacidade: o conhecimento sobre o conteúdo e a execução do contrato deve ser distribuído apenas na medida certa;

d. obrigatoriedade (imposição das regras contratuais): o contrato é executado de forma obrigatória, em sua completude, conforme programado em seu código-fonte, sem margem para interpretações diversas.

O contrato inteligente é executado por envio de mensagem ao endereço do contrato em uma *DLT*, que sinaliza um evento significativo para as regras de negócio que governam as relações entre os participantes do contrato. O papel do intermediário do contrato é delegado à própria tecnologia empregada para o uso de contratos inteligentes, ou seja, a *DLT*. O uso de blocos de dados encadeados, criptografia e algoritmos de consenso, entre outras tecnologias, dá sustentação aos contratos inteligentes.

A utilização de contratos inteligentes provê as seguintes vantagens:

a. transparência: contratos inteligentes podem ser escritos e verificados a qualquer momento por todas as partes envolvidas, que podem verificar o código-fonte do contrato;

b. menor prazo para execução: a eliminação dos passos manuais torna a execução do contrato mais rápida e eficiente;

c. precisão: como o contrato é descrito por um algoritmo computacional, sua execução é precisa, salvo se houver erro de programação;

d. segurança: a infraestrutura de *DLT* garante a segurança em contratos inteligentes, que são assinados por chaves criptográficas e não podem ser violados por terceiros sem permissão de acesso;

e. rastreabilidade: os dados de cada execução das "funções" do contrato ficam armazenados na *DLT*, permitindo que a execução do contrato seja auditável a qualquer tempo;

f. menor custo: por sua natureza digital e em razão da eliminação de intermediários, os contratos inteligentes reduzem os custos de execução;

g. confiança: as características citadas acima levam à maior confiança entre as partes envolvidas no contrato.

2.4 CRIPTOGRAFIA

Soluções baseadas em *blockchain* utilizam intensivamente técnicas tradicionais de criptografia para garantir a integridade das informações armazenadas. Como exemplo, pode-se citar a utilização de algoritmos criptográficos de chaves públicas, funções de *hash* e assinaturas digitais. O detalhamento dessas técnicas está fora do escopo deste relatório, tendo em vista que existem diversos livros e publicações especializados que já tratam sobre o tema.

2.5 *TOKENS*

A tecnologia *blockchain* permite que todo tipo concebível de ativos, direitos e obrigações de dívida, relacionados a bens materiais e imateriais, seja representado por *tokens*, e sua negociabilidade e permutabilidade sejam potencialmente simplificadas.

Desta forma, *tokens* são utilizados para representar ou materializar um ativo do mundo real, ou mesmo um direito, como ações de uma empresa ou um investimento, ou mesmo uma recompensa por um serviço. Os *tokens* podem ser categorizados como:

FIGURA 6 - TIPOS DE TOKENS

Tokens de pagamento
(payment tokens)

São sinônimos de criptomoedas, utilizados tão somente para troca de valores entre partes em uma plataforma de *blockchain*.

Tokens utilitários
(utility tokens)

São *tokens* utilizados para provimento de acesso digital a uma aplicação ou serviço. Representa o direito de acesso, mas não a propriedade de um ativo.

Tokens de ativos
(asset tokens)

Representam ativos do mundo real como ações de uma empresa, direitos de dividendos ou direitos de recebimento de juros sobre um investimento. *Security Tokens* também são *tokens* que representam um ativo sob o ponto de vista de valores mobiliários.

Ressalta-se que os primeiros sistemas de *blockchain*, tais como *Bitcoin* e outras criptomoedas derivadas do *Bitcoin,* são projetos voltados exclusivamente para realizar transferências de valores em moedas digitais, sendo que sua lógica de transação implementa um sistema baseado em *tokens*. A limitação desses sistemas é que apenas registram os saldos digitais associados a identidades ou endereços, juntamente com uma autenticação e as respectivas assinaturas digitais.

Por outro lado, sistemas baseados em contratos inteligentes têm a capacidade de implementar qualquer rotina de *software,* incluindo a lógica de *tokens* digitais. Isso abre a possibilidade para executar, de forma autônoma, lógicas complexas e fluxos de trabalho em código de computador.

2.6 ORÁCULOS

Blockchains e contratos inteligentes funcionam de forma independente do mundo externo e sem necessidade de uma autoridade central. Contudo, especialmente em *blockchains* permissionadas, eventos do mundo exterior podem ter relevância. Assim, pode haver a necessidade de um agente digital que funcione como um intermediário central de confiança sobre fatos externos à rede.

Um oráculo, no contexto de *blockchains*, é um agente que localiza e verifica ocorrências do mundo real e envia essas informações para uma *blockchain*, a fim de serem usadas por contratos inteligentes. Os oráculos fornecem dados externos e acionam execuções de contratos inteligentes quando ocorrem condições pré-definidas.

Importante ressaltar que oráculos são serviços que não fazem parte do mecanismo de consenso da *blockchain*. Em outras palavras, são serviços que verificam ocorrências do mundo físico e enviam essas informações a contratos inteligentes, desencadeando mudanças de estado na *blockchain.*

3_ PRINCIPAIS CARACTERÍSTICAS

HIPER TRANSPARÊNCIA E AUDITABILIDADE

O livro-razão é um dado acessível e público a todos que façam parte da rede, o que significa que os participantes podem ver todo o histórico das transações em tempo real. Essa propriedade da *blockchain* aumenta a rastreabilidade das operações a um grau em que qualquer usuário pode auditar completamente todas as transações. Assim, considerando que, em regra, toda informação do governo deve ser pública, o uso de *blockchain* está aderente à Lei de Acesso à Informação (LAI).

Para um nó participante, essa propriedade aumenta a confiança na rede e reduz comportamentos fraudulentos. Já para o governo, a possibilidade de visualizar *blockchains* públicas das empresas ajuda a monitorar e regular mercados em que não seja um participante direto das operações. Do ponto de vista do cidadão, o fato de poder visualizar quando quiser os dados de *blockchains* governamentais aumenta o controle social sobre as ações da Administração Pública.

INTEGRAÇÃO DE INFORMAÇÕES DENTRO E FORA DOS LIMITES DA ADMINISTRAÇÃO PÚBLICA _DISTRIBUÍDO E DESCENTRALIZADO

Com o uso de uma *blockchain*, os dados são compartilhados em tempo real, além do histórico de modificações, fazendo com que não haja necessidade de reconciliação entre diferentes participantes, uma vez que os dados estão disponíveis a todos os nós e usuários da rede.

Logo, a rede *blockchain* pode ser utilizada como uma camada de integração de bases de dados, permitindo o uso compartilhado entre diversas organizações e colaboradores externos (governo hiper conectado).

DESINTERMEDIAÇÃO E AUTOMAÇÃO DE TRANSAÇÕES E PROCESSOS

A tecnologia *blockchain* introduz um novo paradigma: a possibilidade de diferentes partes transacionarem sem a necessidade de confiar em um intermediário central. A existência de uma terceira parte confiável para resolver conflitos das transações não é mais necessária, pois agora o controle pode ser distribuído para todos os nós da rede de forma descentralizada.

Adicionalmente, reduz a necessidade de implementar processos complexos de reconciliação entre as partes e diminui custos, já que é possível, também, que contratos inteligentes da *blockchain* sejam executados automaticamente, de acordo com regras pré-definidas.

INEXISTÊNCIA DE PONTO ÚNICO DE FALHA _DISPONIBILIDADE

Como todos os participantes têm uma cópia local sincronizada com a rede, se um nó fica indisponível, o livro-razão pode ser acessado através de outros nós. Ou seja, a *blockchain* é uma rede resiliente, com várias cópias compartilhadas de dados, de modo que serviços públicos que necessitam dessas informações podem continuar em operação mesmo que alguns nós não estejam disponíveis.

LOG IMUTÁVEL E INTEGRIDADE DAS INFORMAÇÕES _IMUTABILIDADE E INTEGRIDADE

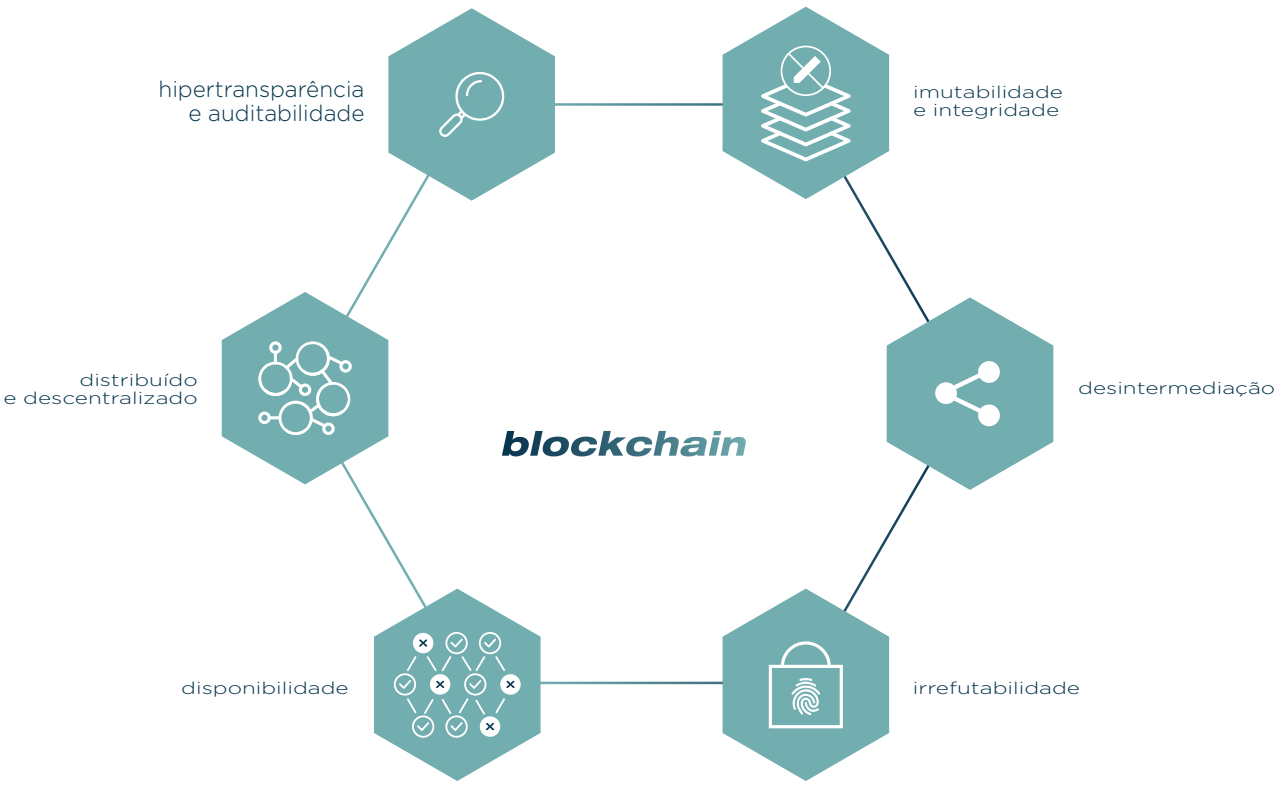
A *blockchain* utiliza técnicas criptográficas para proteger seus registros, incluindo funções de *hash,* ponteiros de *hash* e assinaturas digitais. Isso faz com que qualquer tipo de adulteração seja percebido, por se tratar de uma violação matemática da cadeia de blocos.

Essa propriedade garante que a *blockchain* seja um registro imutável, de forma que nenhuma entidade é capaz de alterar dados passados sem resultar em um alerta à rede e todas as partes podem verificar a consistência dos dados de forma independente.

AUTENTICAÇÃO DAS TRANSAÇÕES _IRREFUTABILIDADE

Uma das funcionalidades essenciais das tecnologias *blockchain* é o uso da criptografia de chaves públicas (ou assimétrica), que serve como uma base para a autenticação dos usuários da rede. Com o uso de um método que utiliza a chave privada do seu par de chaves e funções de *hash,* um participante é capaz de realizar assinaturas digitais sobre as transações, servindo como uma prova inegável de que é o emissor de determinada mensagem (não repúdio).

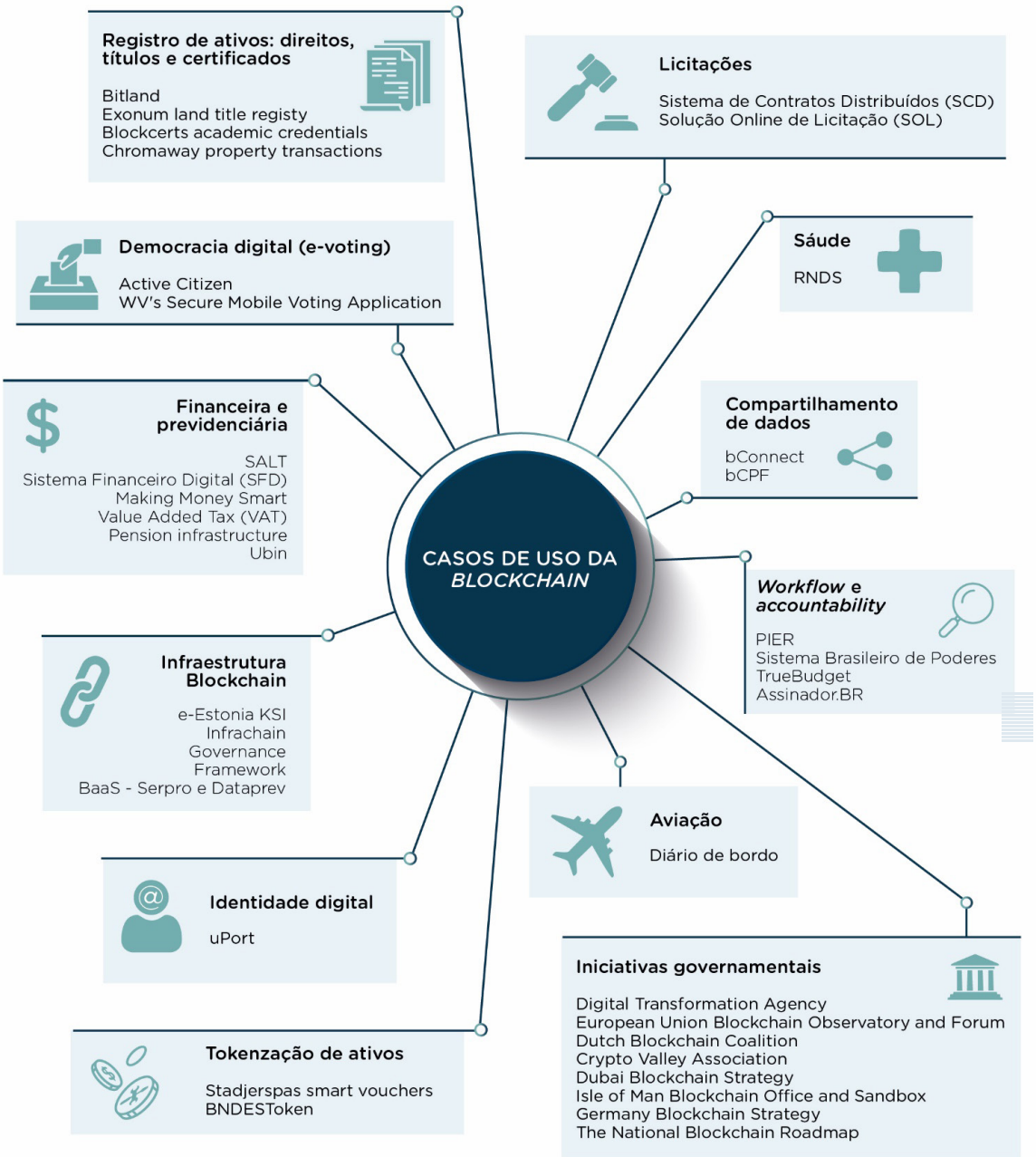
FIGURA 7 - PROPRIEDADES DA TECNOLOGIA *BLOCKCHAIN*



4_ PROJETOS E INICIATIVAS DE APLICAÇÕES *BLOCKCHAIN* E DLTS

O setor público vem adotando a tecnologia distribuída em diversas áreas. O diagrama a seguir exemplifica as áreas de aplicação e respectivos casos de uso da tecnologia *blockchain* que foram identificados no Levantamento realizado pelo TCU.

FIGURA 8 – CASOS DE USO IDENTIFICADOS NO LEVANTAMENTO

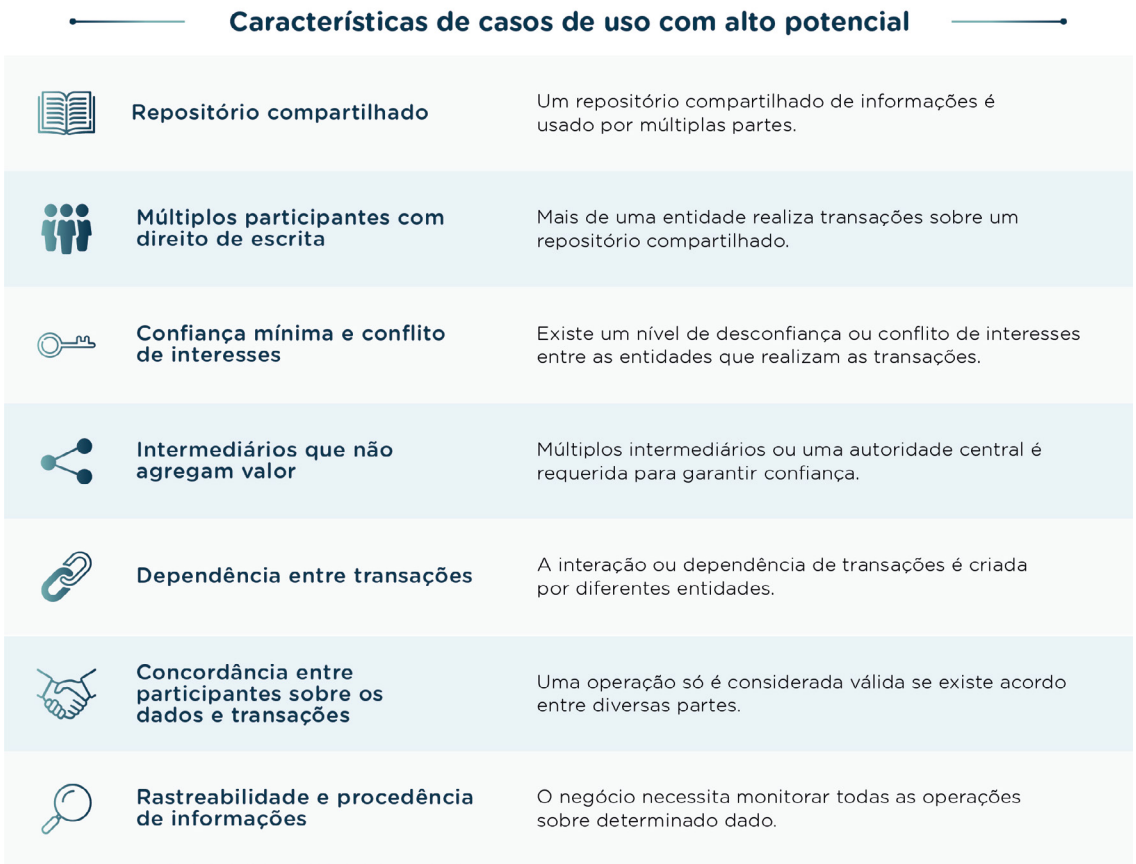


A descrição completa dos projetos identificados pode ser acessada por meio do Apêndice I deste Sumário Executivo.

5_ MODELO DE AVALIAÇÃO DE NECESSIDADES

As tecnologias descentralizadas e distribuídas podem ser aplicadas em áreas que ainda não foram imaginadas. De todo modo, a figura abaixo apresenta características genéricas de casos de uso com alto potencial de se utilizar a tecnologia *blockchain*:

FIGURA 9 - CARACTERÍSTICAS DE CASOS DE USO COM ALTO POTENCIAL

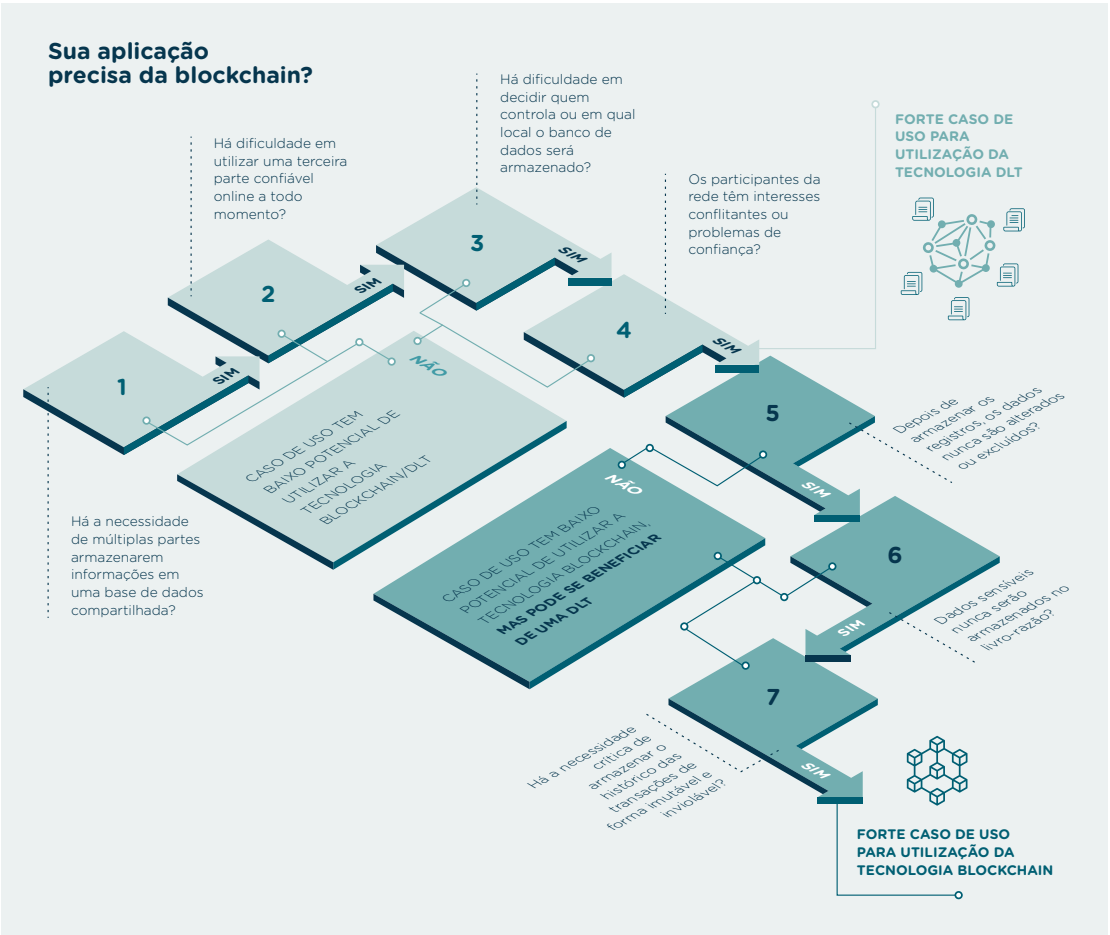


FONTE: FÓRUM ECONÔMICO MUNDIAL (ADAPTADO).

Contudo, como identificar precisamente se uma organização pode se beneficiar de uma solução descentralizada e distribuída? Para decidir se uma solução *blockchain/DLT* se aplica ou não ao caso de uso de uma instituição, apresenta-se um modelo de

avaliação de necessidade, que consiste em perguntas diretas sobre as características do processo de negócio da organização. Quanto mais respostas “sim” nas perguntas de 1 a 7, maior a probabilidade de o caso de uso precisar de uma *DLT*. As perguntas de 5 a 7 referem-se ao caso especial de uma *blockchain*. A imagem abaixo representa o fluxograma mencionado, seguido do detalhamento de cada uma das perguntas.

FIGURA 10 - ÁRVORE DE DECISÃO QUANTO À NECESSIDADE DE UTILIZAR A TECNOLOGIA *BLOCKCHAIN*/DLT



[1] Há necessidade de múltiplas partes armazenarem informações em uma base de dados compartilhada?

Primeiramente, deve-se avaliar se uma ou mais partes têm a necessidade de compartilhar e gravar dados em um mesmo banco de dados. A utilização da tecnologia *blockchain* ou *DLT* requer situações em que múltiplas partes estão envolvidas em uma transação, ou seja, somente faz sentido se existem múltiplos atores e se os dados têm origem em diversas fontes. Caso essa condição não seja verdadeira, o gestor deve avaliar outros tipos convencionais de banco de dados.

[2] Há dificuldade em utilizar uma terceira parte confiável *on-line* a todo momento?

A utilização de uma *blockchain* ou *DLT* envolve a mudança da arquitetura cliente-servidor, frequentemente utilizada pelas aplicações, para o paradigma *P2P*. Caso exista um sistema centralizado que possa resolver determinado problema com elevado grau de disponibilidade, devem ser explicitados os ganhos com a adoção de uma arquitetura distribuída, capaz de garantir a confiabilidade das informações armazenadas. Além disso, deve-se avaliar se existe a necessidade da área de negócio de remover intermediários ou funções burocráticas, uma vez que essas tecnologias favorecem a desintermediação, pelo fato de não dependerem de uma terceira parte confiável.

[3] Há dificuldade em decidir quem controla o banco de dados ou em qual local será armazenado?

Nos sistemas tradicionais, existe desconfiança sobre quem armazena os dados, uma vez que podem ser facilmente manipulados. A arquitetura distribuída resolve o problema quando não há acordo sobre qual participante armazenará as informações. Além disso, como todos os participantes armazenam as mesmas informações, o livro-razão é facilmente auditado pelos nós, aumentando a segurança como um todo. A adoção de uma arquitetura distribuída *blockchain* ou *DLT* pressupõe um modelo de negócio descentralizado, em que múltiplas partes podem ter níveis diferentes de controle dos dados.

[4] Os participantes da rede têm interesses conflitantes ou problemas de confiança?

A utilização da tecnologia *blockchain* é potencializada quando não há confiança mútua entre participantes, uma vez que uma *blockchain* resolve esse problema descentralizando o controle e armazenamento de dados para toda a rede, garantindo que todos os participantes executem as mesmas regras.

[5] Depois de armazenar os registros, os dados nunca são alterados ou excluídos?

Em uma *blockchain*, os dados são armazenados de forma somente escrita, ou seja, novas informações são apenas apensadas, não havendo alteração dos dados que já foram gravados no livro-razão.

[6] Dados sensíveis nunca serão armazenados no livro-razão?

Como os dados são armazenados de forma transparente em toda a rede, a utilização de uma *blockchain* não faz sentido para aplicações que exijam sigilo dos dados. Os nós com acesso à rede podem visualizar e rastrear todo o histórico de transações. Logo, uma *blockchain* deve ser utilizada para armazenamento de dados não sensíveis.

[7] Há necessidade crítica de armazenar o histórico das transações de forma imutável e inviolável?

A imutabilidade e integridade são benefícios essenciais, em virtude de os blocos serem encadeados e armazenados de forma distribuída por nós que seguem as mesmas regras.

Assim, uma *blockchain* é útil quando há necessidade de armazenar, de forma consistente e inviolável, todos os detalhes de transações que foram validadas de acordo com as regras pré-determinadas pela rede, incluindo o *timestamp* e as partes envolvidas.

6_ FATORES CRÍTICOS

Para facilitar as chances de sucesso, as áreas de tecnologia da informação devem levar em consideração os seguintes fatores, antes de implementar projetos de soluções distribuídas.

[1] Conhecimento da tecnologia

Por ser uma tecnologia inovadora, ainda não existem muitos profissionais com habilidades e conhecimento sobre *DLTs.* Por isso, o desenvolvimento de uma aplicação *blockchain* requer capacitação da equipe de TI ou recrutamento de recursos humanos com competência necessária para operar redes distribuídas *peer-to-peer* e escrever contratos inteligentes.

A organização deve conhecer a tecnologia e dominar suas principais características, antes de iniciar um projeto descentralizado, além de estar ciente dos riscos que o uso de uma nova tecnologia pode introduzir.

[2] É necessário justificar o uso (mensurar o impacto para o negócio e o cidadão)

Não se deve adotar uma solução *DLT* por modismo, entusiasmo tecnológico ou em um serviço centralizado que está funcionando bem e tem custo controlado. A organização (ou consórcio) deve saber explicar o porquê de estar adotando o modelo descentralizado e distribuído das tecnologias *blockchain*/*DLT* em determinado caso de uso e como isso impacta em seu negócio e melhora os serviços públicos para o cidadão.

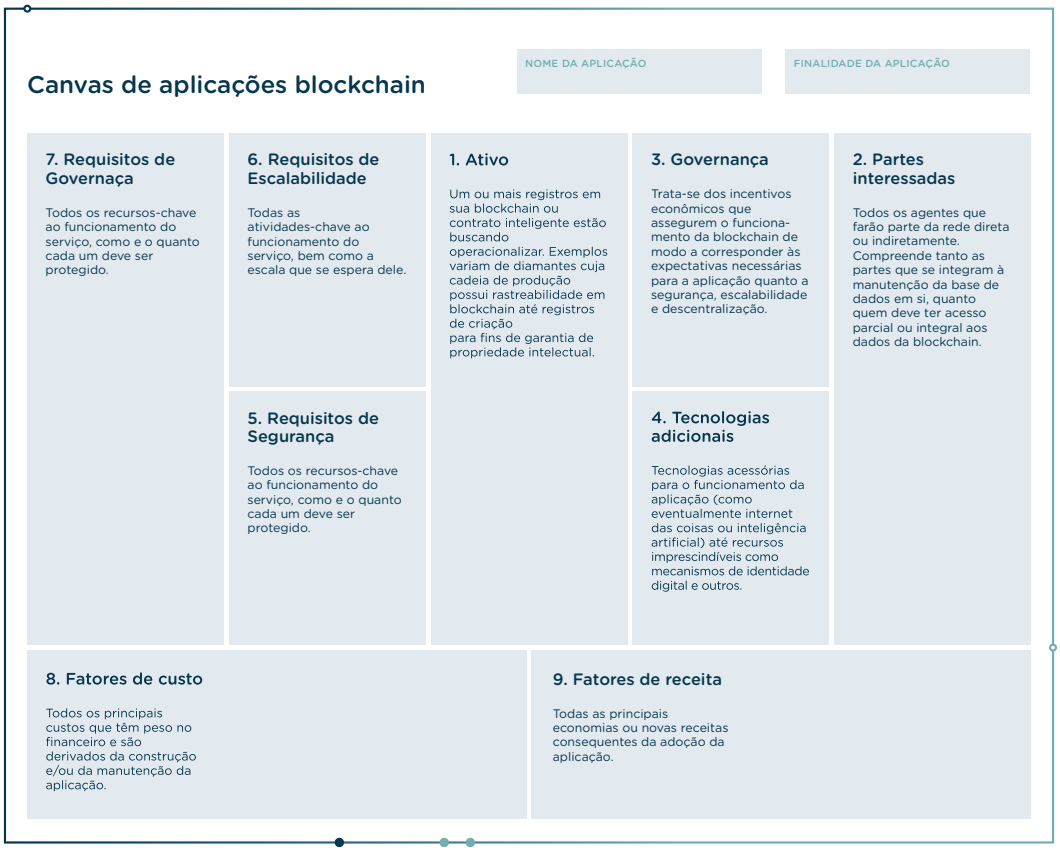
Deve-se avaliar bem o problema que se quer resolver, antes de se optar por uma solução distribuída. Não só isso, espera-se, também, que os profissionais do projeto estejam cientes dos riscos relacionados ao uso da tecnologia, para que possam gerenciá-los de forma efetiva.

Além disso, o novo paradigma requer uma avalição minuciosa sobre o impacto no negócio: quais pessoas, instituições e processos serão afetados? Quais são os ganhos em termos de eficiência e redução de custos que a aplicação pode trazer? Qual é a relação custo-benefício quando comparada a outras tecnologias disponíveis? Como a solução está agregando valor pela perspectiva do cidadão e dos usuários dos serviços? Todas essas perguntas devem ser respondidas de forma clara e objetiva.

Outro ponto de atenção diz respeito ao propósito inicial da tecnologia: a realização de transações sem a necessidade de confiar em uma autoridade central. Assim, a desintermediação é uma propriedade desejável dessa tecnologia quando utilizada nos serviços públicos. Caso existam instituições intermediárias ou funções administrativas que podem ser eliminadas (ou ter sua importância reduzida), elas devem ser explicitadas como benefícios da solução.

A utilização de uma Canvas poderá auxiliar os gestores a fundamentarem a necessidade de utilização da tecnologia *blockchain.*

FIGURA 11 - CANVAS DE APLICAÇÕES *BLOCKCHAIN*



FONTE: INSTITUTO DE TECNOLOGIA E SOCIEDADE DO RIO (ADAPTADO)

[3] Integração com o ambiente computacional e de negócio

Soluções baseadas em *blockchain* quase sempre requerem pontos de integração e/ou interoperabilidade com sistemas legados. Mecanismos de notificação e tratamento de eventos podem ser implementados para fins de atualização de bases de dados legadas e automatização de processos de negócio. Camadas de *software* adicionais, baseadas em *APIs*, podem ser necessárias, para encapsular tanto os sistemas legados quanto a solução *blockchain.*

Em situações de existência de bancos de dados legados, faz-se necessário levar em consideração os possíveis cenários de replicação de dados (a exemplo de cópia ou movimentação de dados da base legada para a *blockchain* e vice-versa), bem como definir quais dados serão armazenados *on-chain* e *off-chain*. Tal definição deve levar em conta, principalmente, os requisitos de confidencialidade, integridade, transparência, rastreabilidade e não repúdio das informações.

[4] Implementação gradual

As tecnologias *blockchain/DLT* ainda estão amadurecendo nas organizações. Portanto, é aconselhável a iniciação da implantação de uma solução distribuída com abordagem experimental, permitindo uma evolução contínua e gradual.

Isso requer a realização de projeto-piloto e provas de conceito com escopo reduzido, para validar o funcionamento da solução e conhecer eventuais obstáculos da tecnologia. A execução de uma fase de experimentação antes de partir para a implementação em larga escala é facilitada pelo fato de estarem disponíveis diversas plataformas de código aberto. Assim, o gestor público pode rapidamente construir um protótipo e validar os requisitos de seu caso de uso sem necessidade de realizar desembolsos elevados.

[5] Os benefícios são potencializados com mais colaboração

As tecnologias *blockchain* movem o poder de uma autoridade central para o consenso baseado em rede. Isso quer dizer que, quanto mais participantes, mais resiliente é uma rede. Além disso, quanto mais entidades fazem uso e contribuem com as informações armazenadas em uma *blockchain,* mais valor a rede possui.

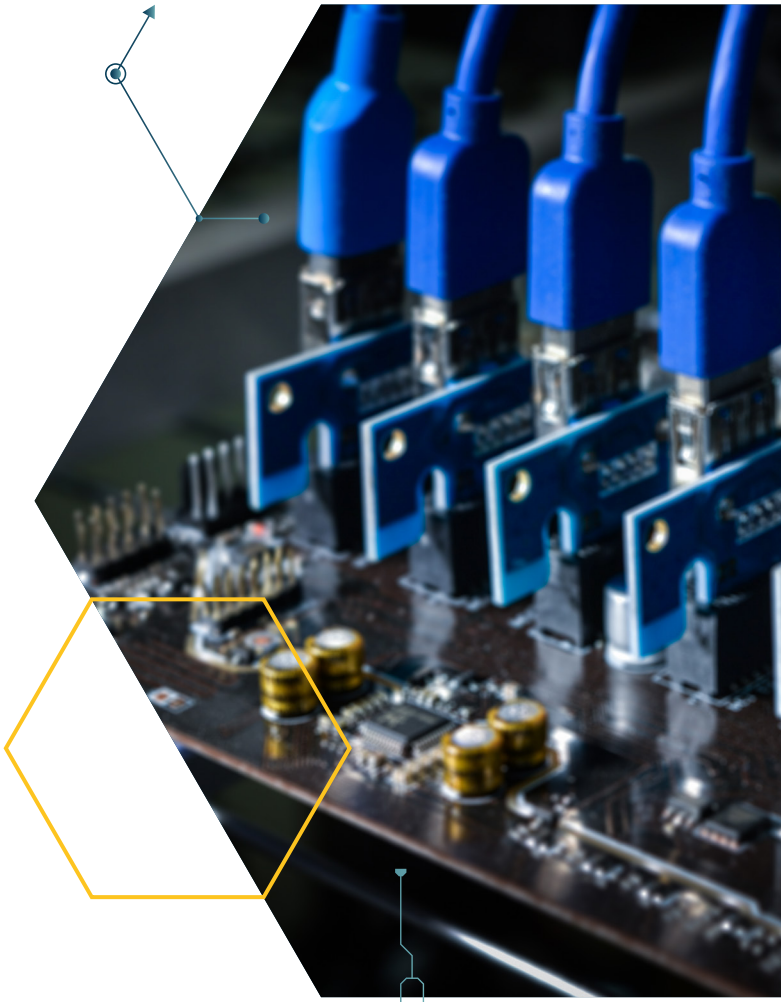
No contexto da Administração Pública, é preciso cooperação e colaboração dos diversos entes para alcançar sucesso com um projeto descentralizado. Assim, deve-se estruturar a governança da rede, com o intuito de identificar principais papéis e responsabilidades relacionados com o problema do caso de uso e garantir que haja mecanismos na solução para incentivar a participação das partes interessadas. Isso permite, também, que haja redução de custos, em razão da natureza descentralizada do projeto.

[6] Estrutura de governança do consórcio adequada

Os projetos de *blockchain* são, por natureza, colaborativos. Isso significa sair de um modelo em que normalmente uma única organização é responsável por administrar os dados para um modelo de negócio em que as decisões do projeto são tomadas por um consórcio de entidades. Assim, criar uma estrutura de governança para organizações colaborativas é fundamental para o sucesso nos projetos de tecnologias distribuídas.

A liderança do consórcio deve definir responsabilidades entre os diferentes níveis de participantes na rede: comitê de governança, usuários, nós colaboradores, operadores técnicos, entre outros atores. Mais ainda, redes complexas podem ter necessidade de definir classes de participantes que podem votar em relação a um assunto específico da rede e se o mecanismo de governança a ser adotado será interno *(on-chain)* ou externo *(off-chain)* à rede *blockchain.*

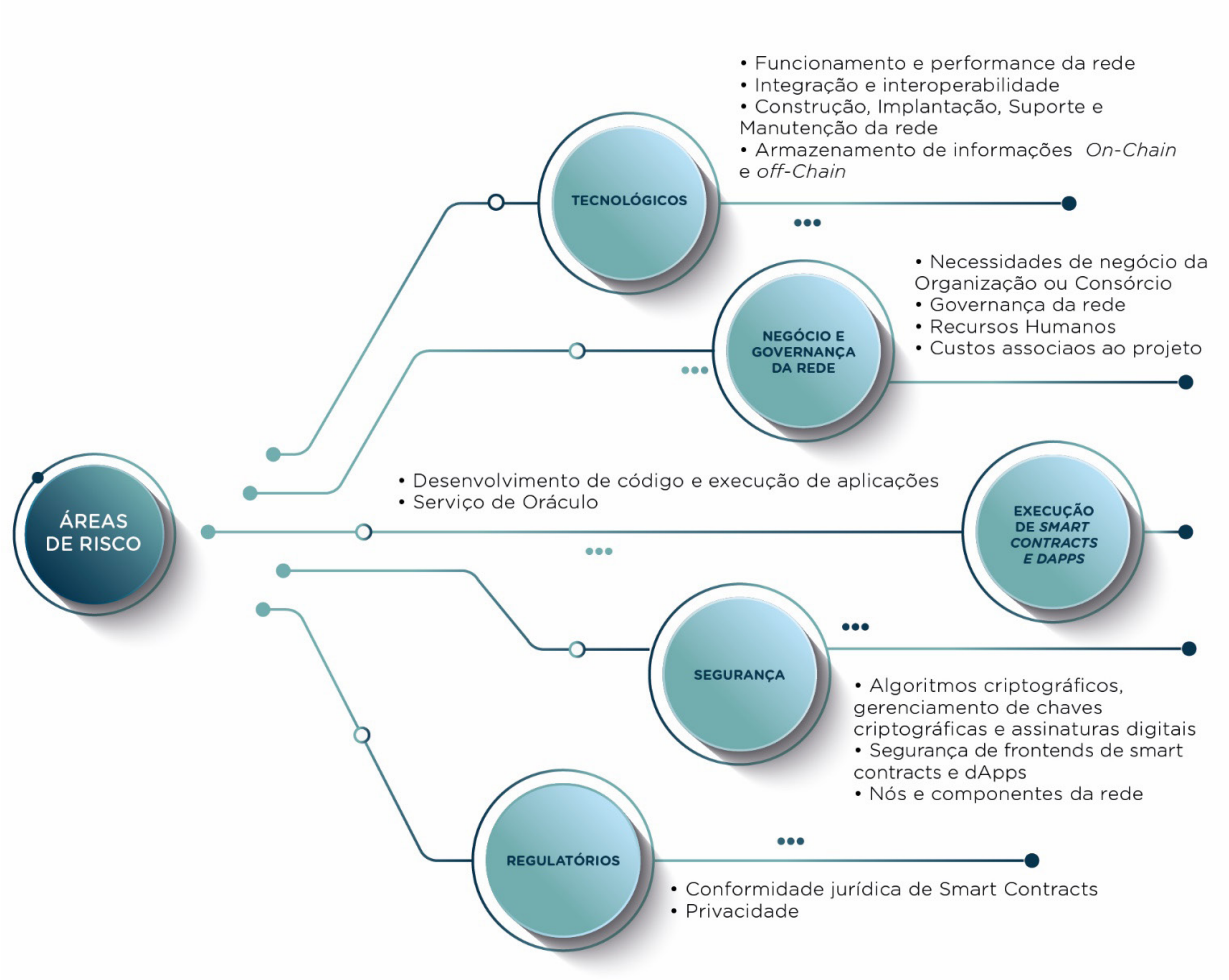
Deve-se garantir que todos os grupos de partes interessadas estejam representados e determinar como as decisões serão tomadas em relação às mudanças na aplicação *blockchain.* Outras questões acessórias também devem ser endereçadas, como, por exemplo, determinar se os direitos dos membros iniciais serão diferentes daqueles dos membros posteriores, de forma que uma rede descentralizada opere de forma sustentável.



7_ RISCOS

Com o surgimento de uma tecnologia emergente, novos riscos também são observados e devem ser tratados. Assim, foi estruturada uma lista contendo possíveis controles associados aos riscos identificados, bem como referências de critérios (normas e boas práticas), com o intuito de auxiliar as áreas de tecnologia da informação das organizações quando forem implementar projetos de *blockchain* e *DLTs.*

FIGURA 12 – ÁREAS DE RISCOS RELATIVOS ÀS TECNOLOGIAS DLTS E *BLOCKCHAIN*



A matriz de risco é apresentada no Apêndice II deste Sumário Executivo.

8_ DESAFIOS E OPORTUNIDADES DAS TECNOLOGIAS BLOCKCHAIN E DLT

[1] Projetos experimentais têm agilidade e baixo custo

Ainda que a experimentação de projetos em *blockchain* precise de um grau elevado de conhecimento de tecnologias distribuídas e programação de contratos inteligentes, devido à natureza *open source* das principais plataformas corporativas de *blockchain* e redes não permissionadas, a Administração Pública pode realizar projetos-piloto para explorar a tecnologia e validar requisitos de forma ágil, sem necessidade de efetuar altos desembolsos para uma solução completa.

[2] DLTs promovem um governo hiperconectado

As tecnologias descentralizadas e distribuídas criam confiança em informações e processos com grandes grupos heterogêneos, sem necessidade de confiar em uma única autoridade central. Isso viabiliza a integração e execução satisfatória de processos, quando há um desnível muito grande entre informações que prestadores de serviço e consumidores detêm sobre determinada transação. No nível mais básico, isso implica serviços públicos aprimorados nos processos de registro e troca de informações.

Em outras palavras, a tecnologia *blockchain/DLT* pode ser usada como uma camada comum e confiável para compartilhamento de informações entre diferentes esferas de governo (municipal, estadual e federal) e países, bem como com a indústria e sociedade. Além do mais, a procedência dessas informações pode ser verificada *on-line*, de modo que o uso compartilhado e confiável de informações poupa tempo e reduz custos para a Administração Pública.

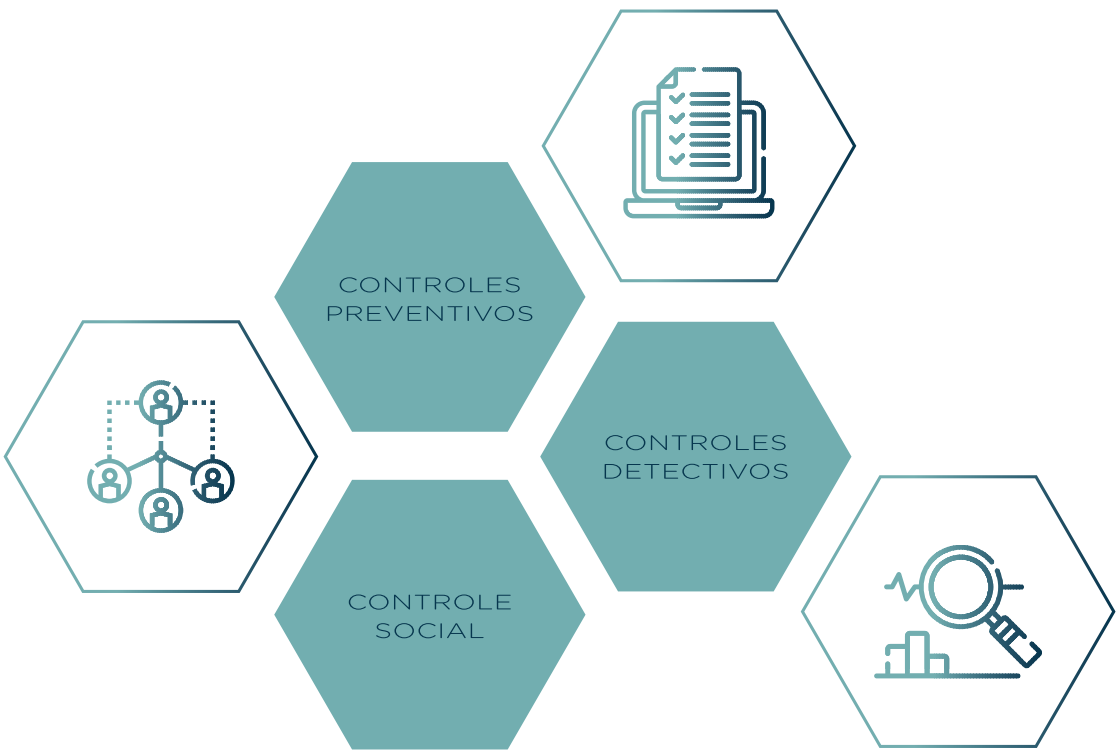
[3] *Blockchain* alinha-se ao combate a fraude e corrupção

A utilização da tecnologia *blockchain/DLT* pode ser considerada tanto um controle preventivo quanto detectivo no combate a fraude e corrupção. A utilização das tecnologias distribuídas permite a criação de trilhas de auditoria para rastrear operações de governo, além de favorecer a abertura de dados. Assim, o fato de cada participante da rede manter seu próprio registro atualizado das transações aumenta a transparência e reduz as oportunidades de fraude, dificultando a ocorrência de delitos e comportamentos antiéticos.

Além disso, como o *hash* de uma transação é vinculado aos *hashes* de todas as transações anteriores, as transações passadas podem ser verificadas e investigadas, de modo que as tentativas de adulteração são perceptíveis para os participantes da rede. Assim, a tecnologia também funciona como um controle detectivo, possibilitando rastreio e identificação de atividades ilegais.

O gerenciamento de dinheiro público é uma área em que soluções *blockchain* podem ajudar a minimizar fraudes e aumentar a transparência e responsabilidade dos entes envolvidos. Por exemplo, com a utilização de contratos inteligentes, é possível estabelecer que repasses de determinado programa de governo sejam efetivamente realizados somente se a transação for legítima, considerando parâmetros como valor, beneficiários, temporalidade, área de aplicação do recurso, entre outros.

Sendo assim, nota-se o potencial da tecnologia *blockchain* para prevenir e detectar desvios simultaneamente, em decorrência de suas características inerentes (transparência, imutabilidade e irrefutabilidade), promovendo, assim, a cultura da prestação de contas nos serviços públicos e na realização das despesas governamentais. Todas essas vantagens reunidas aumentam a confiança nos dados mantidos pelo governo, especialmente nos casos em que cidadãos desconfiam da veracidade das informações, promovendo assim um controle social efetivo.



[4] *Blockchain* otimiza serviços digitais prestados ao cidadão

Os processos intra-organizacionais enfrentam desafios de governança e desconfiança entre organizações, que impedem sua otimização. Além disso, a falta de um entendimento comum da lógica do processo pode ser um complicador na prestação de serviços que dependam da colaboração de vários órgãos.

A tecnologia *blockchain* permite que os processos sejam executados de maneira distribuída, sem delegar confiança às autoridades centrais nem exigir confiança mútua entre os participantes. Desta maneira, a capacidade de realizar transações sem a necessidade de uma terceira parte confiável tem o potencial de desintermediar funções e instituições de governo.

Portanto, os serviços digitais que envolvem diferentes órgãos do governo podem ser beneficiados pela arquitetura descentralizada da *blockchain.* Especificamente, um modelo de processo que compreenda tarefas executadas por várias partes pode ser coordenado e automatizado por meio de contratos inteligentes em uma rede *blockchain.* As vantagens mais importantes dos contratos inteligentes são que eles contêm um registro transparente e à prova de violações das transações, em que nenhum terceiro é necessário para garantir a confiança.

Contratos inteligentes podem ser implementados para otimizar serviços digitais em que: há trabalho manual para verificar dados objetivos ou quantificáveis; as partes não se conhecem ou não confiam uma na outra; existem interesses conflitantes; se exige confiança e transparência; os dados podem ser verificados, automaticamente, em fontes confiáveis. Além disso, a tecnologia *blockchain* também pode ajudar os governos a reduzir os erros e o custo de processos que exigem muita interferência humana.

Por fim, considerando os recursos atualmente gastos na verificação e reconciliação dos dados coletados pela Administração Pública, espera-se uma substancial economia de custo e tempo, que pode ser obtida via *blockchain* de maneira descentralizada e em tempo real, reduzindo, assim, a redundância de controles.

[5] Papel do governo na prestação de serviços digitais é redefinido

No futuro, a função de autoridade centralizada exercida pelo governo pode se tornar menos relevante no contexto das tecnologias *blockchain* ou seu papel pode mudar, para fornecer plataforma e governança para serviços descentralizados, em vez de estar no centro de todas as transações. Essa será uma oportunidade para que processos colaborativos sejam redefinidos, possibilitando o surgimento de novos arranjos institucionais que façam uso extensivo de transações digitais inovadoras, propiciando que plataformas *blockchain* mantidas pelo governo conectem diferentes partes interessadas e criem valor público para desenvolvimento da economia.

O governo poderá desempenhar o papel de um administrador confiável que inicia e opera um registro, determina as regras de transação e audita os aplicativos para garantir o funcionamento adequado. No papel de gestor dos dados, o governo provavelmente permanecerá responsável pela configuração, operação e manutenção das aplicações e poderá ser responsabilizado em caso de falha ou quando houver problemas com a qualidade dos dados. Como tal, a tecnologia descentralizada exigirá uma reintermediação dos papéis do governo.

Assim, há a possibilidade de reduzir ainda mais as atribuições do governo. Em um possível cenário, a Administração Pública possivelmente não precisará mais fornecer, por conta própria, processos de armazenamento e troca de informações que facilitam as atividades econômicas na sociedade, uma vez que isso poderá ser totalmente feito pelo protocolo *blockchain.* Nessa situação, o governo deverá manter um papel de supervisão, no que diz respeito às transações que ocorrem nessa infraestrutura.

[6] Projetos *blockchain* no âmbito da Administração Pública Federal ainda estão em estágio de experimentação

A despeito de todo esforço empreendido por várias organizações, no âmbito da Administração Pública Federal, os projetos *blockchain* analisados durante esta auditoria ainda estão em experimentação, ou em estado inicial de produção, envolvendo um pequeno número de participantes. De fato, não há, no momento da escrita deste relatório, nenhuma aplicação *blockchain* sendo utilizada em larga escala no âmbito da Administração Pública federal. Logicamente, essa situação poderá ser modificada, à medida que a tecnologia amadureça, os projetos tenham o crescimento esperado em número de transações e participantes e as experiências de casos de sucesso sejam compartilhadas entre as organizações.

[7] Aplicações *blockchain* no âmbito da Administração Pública Federal não envolvem diretamente o cidadão brasileiro

As iniciativas *blockchain* na Administração Pública Federal ainda não alcançaram diretamente o cidadão brasileiro. As aplicações observadas, em sua maioria, são voltadas à colaboração entre entidades públicas e privadas, sem a participação de pessoa física. Em outros países, verifica-se a interação dos cidadãos diretamente em aplicações *blockchain.* A visibilidade pública e possibilidade de interação direta do cidadão, além de ter efeito positivo na prestação dos serviços digitais, aumenta o controle social. Assim, entende-se que as aplicações que utilizam a tecnologia *blockchain* na Administração Pública podem e devem ser um instrumento de participação direta do cidadão brasileiro nas mais diversas questões, promovendo maior transparência e diminuição da burocracia estatal.

[8] Plataformas *blockchain* permissionadas ainda não estão consolidadas

As plataformas de *blockchain* permissionadas, como a *Quorum e Hyperledger,* entre outras, ainda são relativamente novas, a despeito de terem tido uma evolução rápida. Tais ferramentas ainda não estão consolidadas e, em alguns casos, componentes importantes poderão ser alterados ou evoluídos, causando descontinuidade das tecnologias adotadas nas aplicações já desenvolvidas.

Há notícias, por exemplo, da troca de mecanismos de consenso entre versões de uma determinada plataforma e, vale lembrar, tal mecanismo é componente central de uma plataforma *blockchain.* Assim, nota-se que as plataformas permissionadas ainda estão em consolidação, o que envolve risco de manutenções custosas, ou mesmo descontinuidade, em aplicações já desenvolvidas ou em desenvolvimento.

Outro ponto que merece atenção é que as plataformas permissionadas não têm especificações mundialmente reconhecidas acerca da tecnologia *blockchain.* A despeito do esforço da comunidade europeia e do *International Telecommunication Union (ITU)* na padronização e disseminação do conhecimento sobre *blockchain,* ainda não há um consenso sobre termos e padronizações em torno das ferramentas de mercado. De fato, plataformas observadas definem termos próprios e tecnologias próprias em suas implementações. A falta de padronização e especificação pode levar ao efeito *vendor lock-in,* em que a adoção de uma plataforma ou um produto torna o cliente refém desta escolha.

[9] Não há interoperabilidade entre plataformas *blockchain*

No momento da escrita deste relatório, as plataformas de *blockchain* permissionadas, a princípio, não são interoperáveis, o que significa dizer que os dados persistidos em uma plataforma não são intercambiáveis entre plataformas *blockchain.* Isso dificulta sobremaneira a colaboração entre aplicações *blockchain*, impedindo muitas vezes que um processo de negócio possa ser executado pela colaboração entre órgãos que usam diferentes plataformas *blockchain* em suas aplicações. Tal lacuna tem sido suprida pelo desenvolvimento de *APIs* e pelo registro de dados *off-chain.*

[10] Existem poucos profissionais com conhecimento sobre a tecnologia *blockchain* no âmbito da Administração Pública Federal

Por ser uma tecnologia relativamente nova, o número de profissionais e servidores com domínio dos aspectos técnicos e conceitos que envolvem *blockchain* ainda é baixo, pelo menos nas organizações estatais visitadas no âmbito desta auditoria. Consta que, em órgãos e empresas específicas da Administração Pública, o domínio ainda está sob tutela de entusiastas da tecnologia *blockchain.*

Além disso, há poucos programadores disponíveis no mercado com conhecimento suficiente para escrever código de contratos inteligentes, o que pode ser um limitador na adoção dessa tecnologia pelo governo.

[11] Sistema de identidade digital pode viabilizar o uso massivo da tecnologia *blockchain*

De acordo com o *The European Union Blockchain Observatory & Forum,* um dos requisitos mais importantes na construção de uma sociedade digital é a disponibilização de uma identidade digital viável para todos os cidadãos, as empresas, os órgãos públicos ou, cada vez mais, as máquinas e outros agentes autônomos. A organização refere-se à ideia de criação de uma identidade auto-soberana, baseada em *blockchain,* em que, ao invés de os indivíduos manterem suas informações de identificação com terceiros, os próprios indivíduos seriam capazes de guardar suas informações de identificação autenticadas.

No paradigma da auto-soberania, os governos podem, por exemplo, emitir certificados assinados digitalmente para seus cidadãos ou residentes, atestando o nome, o endereço, a data de nascimento, o local de nascimento da pessoa, a residência, a permissão de dirigir, as propriedades imobiliárias, o título de eleitor e assim por diante. Sob esse paradigma, os indivíduos seriam, pelo menos, em teoria, responsáveis por proteger seus próprios dados pessoais.

9_ CONCLUSÃO

A *blockchain*, tecnologia subjacente do *bitcoin*, surgiu em 2008 com o propósito de permitir que os participantes da rede realizassem transações monetárias na internet sem a necessidade de confiar em uma autoridade central. As transações registradas no livro-razão são públicas, de modo que tentativas de violação das informações são facilmente identificadas.

Assim, rapidamente, essa tecnologia despertou o interesse da comunidade digital e houve um forte desenvolvimento colaborativo no sentido de aprimorar suas funcionalidades. No atual cenário, incorporou-se à tecnologia *blockchain* a capacidade de executar contratos inteligentes, os quais permitem que as partes concordem previamente sobre os termos de um acordo e ele seja cumprido automaticamente, sem a necessidade de coordenação ou intervenção humana nem da atuação de uma terceira parte confiável.

Essa tecnologia também permite uma nova forma de representar situações da vida real, de modo que pode se tornar uma ferramenta poderosa para rastreamento de transações que ajudam na redução da corrupção e no aumento da confiança dos usuários, levando ao aprimoramento dos serviços públicos digitais.

Embora a tecnologia *blockchain* tenha se popularizado com o uso de criptomoedas, esse é somente um exemplo de como as tecnologias distribuídas de livro-razão podem ser utilizadas. Dentre as diversas áreas em que a *blockchain* pode ser aplicada na ampliação e melhoria de serviços do Governo, elencam-se o processo tributário, a universalização de serviços de saúde, a criação de identidades digitais auto-soberanas, a gestão de convênios, a inclusão digital dos desbancarizados, o acompanhamento de repasses financeiros, a desintermediação de serviços cartoriais, a implantação de um processo eleitoral mais robusto e a prevenção à fraude e à lavagem de dinheiro.

Atualmente diversos países e organizações, entre eles o Brasil, estão prospectando soluções e desenvolvendo projetos baseados em *blockchain* para auxiliar a resolver alguns de seus problemas de negócio. Os benefícios da tecnologia para o setor público são a capacidade do governo prestar serviços com maior eficiência e segurança, automação aprimorada, transparência e auditabilidade, beneficiando assim a sociedade.

Dessa forma, em um mundo em que cidadãos e empresas não dependem de intermediários para registrar informações e contratos inteligentes substituem controles manuais, nota-se que a automação e a confiança provida por soluções em *blockchain* poderá ser um instrumento poderoso no desafiador processo de transformação digital, uma vez que a tecnologia *blockchain* oferece a oportunidade de criar novas maneiras de colaboração por meio da descentralização.

Nesse contexto, é relevante que os agentes públicos conheçam outros projetos e casos de uso, compreendam os benefícios e os riscos inerentes à tecnologia *blockchain*, bem como os principais fatores críticos de sucesso para que possam avaliar a pertinência da implantação de projetos em *blockchain* para sua organização.

Portanto, com o intuito de auxiliar gestores públicos na difícil missão da transformação digital, com eficiência e segurança, o presente sumário executivo consolidou informações do Levantamento do TCU sobre a tecnologia emergente *blockchain*, apresentando *framework* projetado para promover a cultura da inovação e ajudar as organizações a empreenderem novos projetos baseados em tecnologias descentralizadas e distribuídas no país.

10_ REFERÊNCIAS

ALEMANHA. Bundesministerium der Finanzen. Blockchain Strategy of the Federal Government: We Set Out the Course for the Token Economy. Disponível em: <https://www.bmwi.de/Redaktion/EN/Publikationen/Digitale-Welt/blockchain-strategy.pdf?__blob=publicationFile&v=3>. Acesso em: 11 dez. 2019.

ALLESSIE, David; SOBOLEWSKI, Maciej; VACCARI, Lorenzino. Joint Research Centre (JRC). Blockchain for digital government: An assessment of pioneering implementations in public services. Luxemburgo: Publications Office Of The European Union, 2019. Disponível em: <http://publications.jrc.ec.europa.eu/repository/bitstream/JRC115049/blockchain_for_digital_government_online.pdf>. Acesso em: 5 set. 2019.

ANTONOPOULOS, Andreas M. A Internet do Dinheiro. São Paulo: Rede Editora, 2018. 124 p. (Volume 1).

Australian Governament. National blockchain roadmap. Disponível em: https://www.industry.gov.au/sites/default/files/2020-02/national-blockchain-roadmap.pdf. Acesso em: 11 mar. 2020.

BERRYHILL, Jamie; BOURGERY, Théo; HANSON, Angela. Blockchains Unchained: Blockchain Technology and its Use in the Public Sector. Oecd Working Papers On Public Governance n. 28, 2018. 53 p. http://dx.doi.org/10.1787/3c32c429-en

BNDES. II Fórum BlockchainGov. Disponível em: <https://bndes.gov.br/wps/portal/site/home/conhecimento/seminarios/II-forum-blockchaingov>. Acesso em: 10 jan. 2020.

BUTERIN, Vitalik. A next-generation smart contract and decentralized application platform. 2014. Disponível em: <http://blockchainlab.com/pdf/Ethereum_white_paper-a_next_generation_smart_contract_and_decentralized_application_platform-vitalik-buterin.pdf>. Acesso em: 11 dez. 2019.

CANADÁ. Chamber Of Digital Commerce. Canadian Blockchain Census 2019: Part I: Measuring Canada's Blockchain Ecosystem. 2019. Disponível em: <https://www.blockchainresearchinstitute.org/wp-content/uploads/2019/10/Chamber-Blockchain-Census-2019.pdf>. Acesso em: 8 nov. 2019.

CHICARINO, et al. O uso de Blockchain para Privacidade e Segurança em Internet das Coisas. Livro de minicursos do XVII Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais (SBSeg'17), Brasília-DF. 2017. p. 99–148. Disponível em: <https://sbseg2017.redes.unb.br/wp-ontent/uploads/2017/04/20171107-SBSeg2017-Livro_de_Minicursos.pdf>. Acesso em 21 nov. 2019.

CLAYTON, J. Securities and Exchange Commission (SEC). Statement on Cryptocurrencies and Initial Coin Offerings. Disponivel em: <https://www.sec.gov/news/public-statement/statement-clayton-2017-12-11>. Acesso em: 19 set. 2019.

Data Foundation. Bringing Blockchain Into Government: a path forward for creating effective federal blockchain initiatives. 2019. Disponível em: <https://www.datafoundation.org/bringing-blockchain-into-government>. Acesso em: 8 nov. 2019

Food And Agriculture Organization of The United Nations (FAO) and The International Telecommunication Union (ITU). E-Agriculture in action: Blockchain for agriculture - Opportunities and Challenges. 2018. Disponível em: http://handle.itu.int/11.1002/pub/8129545a-en. Acesso em: 12 fev. 2020.

GREVE, Fabíola, et al. Blockchain e a Revolução do Consenso sob Demanda. In Minicursos do XXXVI do Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuıdos (SBRC), São Carlos-SP. 2018. 52 p. Disponível em: <http://www.sbrc2018.ufscar.br/wp-content/uploads/2018/04/Capitulo5.pdf>. Acesso em: 11 dez. 2019.

HEWETT, Nadia; LEHMACHER, Wolfgang; WANG, Yingli. World Economic Forum. Inclusive Deployment of Blockchain for Supply Chains: Part 1 – Introduction. 2019. Disponível em: <http://www3.weforum.org/docs/WEF_Introduction_to_Blockchain_for_Supply_Chains.pdf>. Acesso em: 8 out. 2019.

HOMAN FARAHMAND. Gartner. Guidance for Assessing Blockchain Platforms. Disponível em: <https://www.gartner.com/en/documents/3905773/guidance-for-assessing-blockchain-platforms>. Acesso em: 18 set. 2019.

HOULGATE, Rick; FURLONGER, David; HOWARD, Rick. Gartner. Evaluate Promising and Maturing Blockchain Use Cases in Government. 2019. Disponível em: <https://www.gartner.com/en/documents/3913384/evaluate-promising-and-maturing-blockchain-use-cases-in->. Acesso em: 21 nov. 2019.

Instituto De Tecnologia & Sociedade do Rio. Relatório Blockchain para aplicações de interesse pú-

blico. Disponível em: https://itsrio.org/wp-content/uploads/2019/03/Relat%C3%B3rio-ITS-GE-Blockchain-vFinal.pdf. Acesso em: 12 nov. 2019.

International Monetary Fund. Treatment of Crypto Assets in Macroeconomic Statistics. Disponível em: <https://www.imf.org/external/pubs/ft/bop/2019/pdf/Clarification0422.pdf>. Acesso em: 6 nov. 2019.

ITU-T FOCUS GROUP ON APPLICATION OF DISTRIBUTED LEDGER TECHNOLOGY (FG DLT). Technical Report FG DLT D2.1: Distributed ledger technology terms and definitions. 2019. Disponível em: <https://www.itu.int/en/ITU-T/focusgroups/dlt/Documents/d11.pdf>. Acesso em: 9 dez. 2019.

ITU-T FOCUS GROUP ON APPLICATION OF DISTRIBUTED LEDGER TECHNOLOGY (FG DLT). Technical Report FG DLT D2.1: Distributed ledger technology use cases. 2019. Disponível em: <https://www.itu.int/en/ITU-T/focusgroups/dlt/Documents/d21.pdf>. Acesso em: 9 dez. 2019.

ITU-T FOCUS GROUP ON APPLICATION OF DISTRIBUTED LEDGER TECHNOLOGY (FG DLT). Technical Report FG DLT D3.3: Assessment criteria for distributed ledger technology platforms. 2019. Disponível em: <https://www.itu.int/en/ITU-T/focusgroups/dlt/Documents/d33.pdf>. Acesso em: 18 set. 2019.

Joint Research Centre (JRC). Blockchain now and tomorow: assessing multidimensional impacts of distributed ledger technologies (Executive Sumary). 2019. Disponível em: https://publications.jrc.ec.europa.eu/repository/bitstream/JRC117255/blockchain_executive-summary_online.pdf. Acesso em: 6 fev. 2020.

KANE, Ethan. Is Blockchain a General Purpose Technology? 2017. Disponível em: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2932585>. Acesso em: 8 out. 2019.

KPMG. Auditing blockchain solutions. Disponível em: <https://assets.kpmg/content/dam/kpmg/in/pdf/2018/10/Auditing_Blockchain_Solutions.pdf>. Acesso em: 18 set. 2019.

MITRA, R. Utility Tokens vs Security Tokens: Learn The Difference – Ultimate Guide. Disponivel em: <https://blockgeeks.com/guides/utility-tokens-vs-security-tokens/>. Acesso em: 25 set. 2019.

MULLIGAN, Catherine et al. Blockchain Beyond the Hype: A Practical Framework for Business Leaders. World Economic Forum .2018. Disponível em: <http://www3.weforum.org/docs/48423_Whether_Blockchain_WP.pdf>. Acesso em: 8 out. 2019.

NAKAMOTO, Satoshi. Bitcoin: A peer-to-peer eletronic cash system. 2008. Disponível em: <https://bitcoin.org/bitcoin.pdf>. Acesso em: 5 set. 2019.

OECD. The Tokenisation of Assets and Potential Implications for Financial Markets. Disponível em: <https://www.oecd.org/finance/The-Tokenisation-of-Assets-and-Potential-Implications-for-Financial--Markets.pdf>. Acesso em: 11 fev. 2020.

ØLNES, Svein; UBACHT, Jolien; JANSSEN, Marijn. Blockchain in government: Benefits and implications of distributed ledger technology for information sharing. Government Information Quarterly, [s.l.], v. 34, n. 3, p.355-364, set. 2017. Elsevier BV. http://dx.doi.org/10.1016/j.giq.2017.09.007.

REVOREDO, Tatiana. Blockchain: Tudo O Que Você Precisa Saber. Independently Published, 2019. 408 p.

Satoshi Nakamoto. In: Wikipédia. Disponível em: <https://en.wikipedia.org/wiki/Satoshi_Nakamoto>. Acesso em 9 out. 2019.

STAMPLES, M. et al. Commonwealth Scientific and Industrial Research Organisation (CSIRO). Risks and opportunities for systems using Blockchain and Smart Contracts. 2017. Disponível em: <https://www.data61.csiro.au/~/media/052789573E-9342068C5735BF604E7824.ashx>. Acesso em: 8 nov. 2019.

Swiss Financial Market Supervisory Authority (FINMA). FINMA publishes ICO guidelines. Disponivel em: <https://www.finma.ch/en/news/2018/02/20180216-mm-ico-wegleitung/>. Acesso em: 19 set. 2019.

Symbiont. Smart contract vs “token”-based systems. Disponível em: <https://medium.com/symbiont-io/smart-contract-vs-token-based-systems-ccdd99af41e3>. Acesso em: 11 nov. 2019.

SZABO, N. Smart Contracts: Building Blocks for Digital Markets, 1996. Disponivel em: http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_2.html. Acesso em: 12 set. 2019.

The European Union Blockchain Observatory & Forum. Blockchain for Government and Public Services. 2018. Disponível em: <https://www.eublockchainforum.eu/sites/default/files/reports/eu_ob-

servatory_blockchain_in_government_services_v1_2018-12-07.pdf>. Acesso em: 5 set. 2019.

Vitalik Buterin. In: Wikipédia. Disponível em: <https://en.wikipedia.org/wiki/Vitalik_Buterin>. Acesso em 9 out. 2019.

YAGA, Dylan et al. NISTIR 8202: Blockchain Technology Overview. 2018. https://doi.org/10.6028/NIST.IR.8202

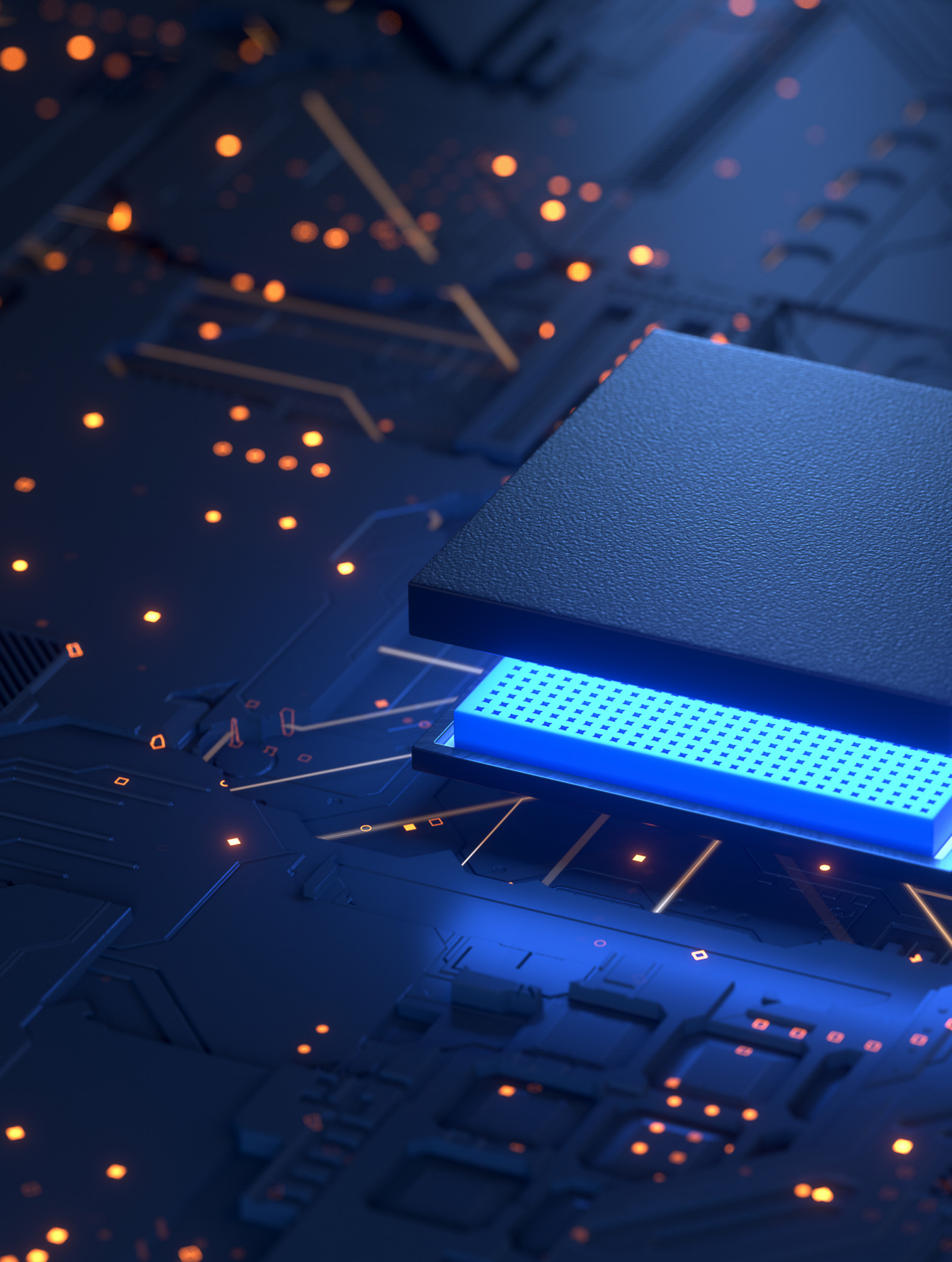
BNDES. **II Fórum BlockchainGov.** Disponível em: <https://bndes.gov.br/wps/portal/site/home/conhecimento/seminarios/II-forum-blockchaingov>. Acesso em: 10 jan. 2020.

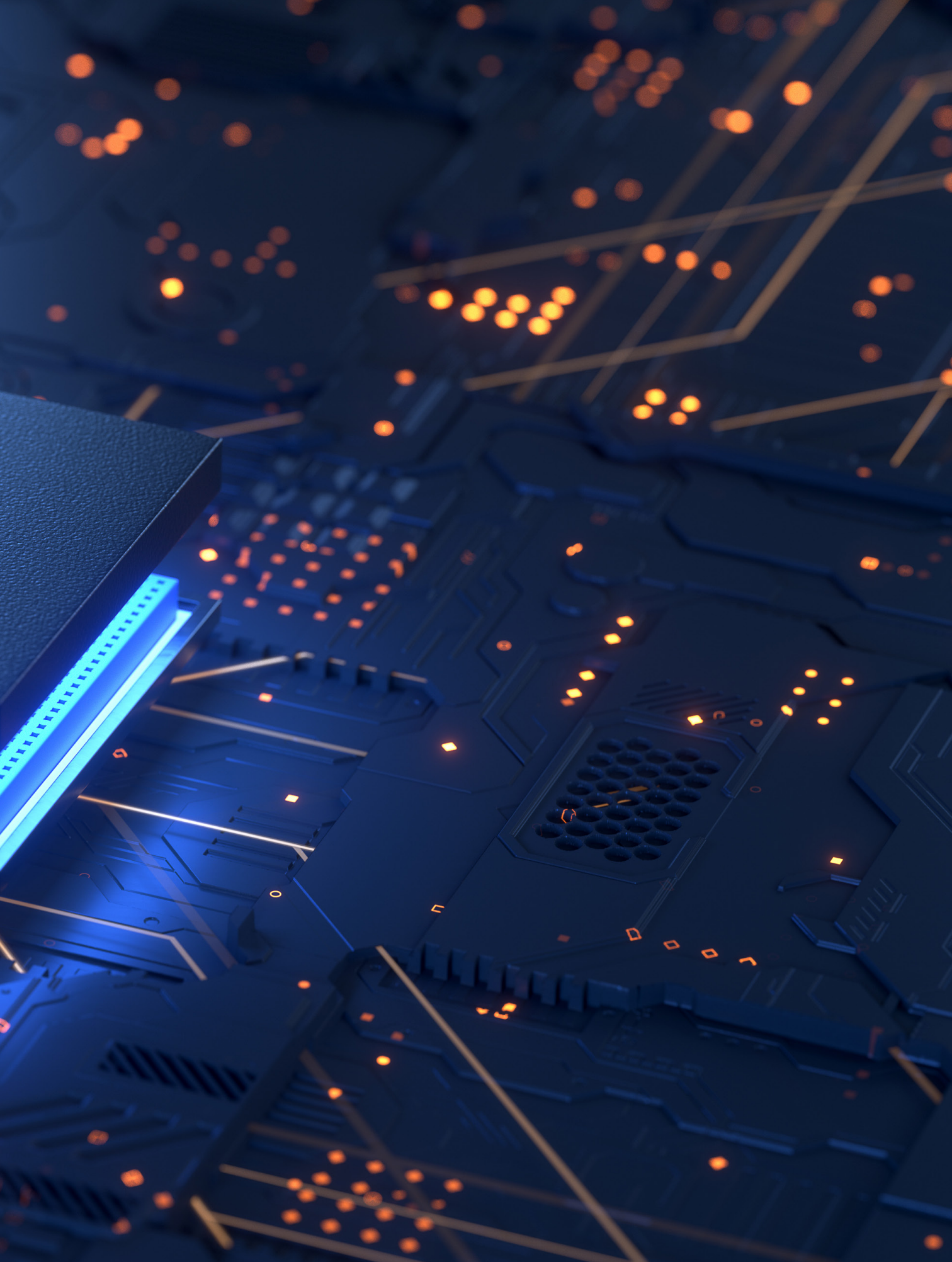
HOMAN FARAHMAND. Gartner. **Guidance for Assessing Blockchain Platforms.** Disponível em: <https://www.gartner.com/en/documents/3905773/guidance-for-assessing-blockchain-platforms>. Acesso em: 18 set. 2019.

ITU-T FOCUS GROUP ON APPLICATION OF DISTRIBUTED LEDGER TECHNOLOGY (FG DLT). **Technical Report FG DLT D3.3:** Assessment criteria for distributed ledger technology platforms. 2019. Disponível em: <https://www.itu.int/en/ITU-T/focusgroups/dlt/Documents/d33.pdf>. Acesso em: 18 set. 2019.

KPMG. **Auditing blockchain solutions.** Disponível em: <https://assets.kpmg/content/dam/kpmg/in/pdf/2018/10/Auditing_Blockchain_Solutions.pdf>. Acesso em: 18 set. 2019.

Instituto De Tecnologia & Sociedade do Rio. Relatório Blockchain para aplicações de interesse público. Disponível em: https://itsrio.org/wp-content/uploads/2019/03/Relat%C3%B3rio-ITS-GE-Blockchain-vFinal.pdf. Acesso em: 12 nov. 2019.





Responsabilidade pelo conteúdo
Secretaria-Geral da Presidência (Segepres)
Secretaria das Sessões (Seses)

Projeto gráfico, diagramação e capa
Secretaria de Comunicação (Secom)
Núcleo de Criação e Editoração (NCE)

Tribunal de Contas da União
Secretaria-Geral da Presidência (Segepres)
SAFS Quadra 4 Lote 1
Edifício Sede Sala 146
70.042-900, Brasília – DF
(61) 3316-5338
segepres@tcu.gov.br

Ouvidoria do TCU
0800 644 1500
ouvidoria@tcu.gov.br

Impresso pela Senge/Segedam

TRIBUNAL DE CONTAS DA UNIÃO

_Missão

Aprimorar a Administração Pública em benefício da sociedade por meio do controle externo.

_Visão

Ser referência na promoção de uma Administração Pública efetiva, ética, ágil e responsável.

www.tcu.gov.br